Groupe de travail Réseau
Request for Comments : 3856
Catégorie : En cours de normalisation

J. Rosenberg, dynamicsoft
août 2004
Traduction Claude Brière de L'Isle

Paquetage d'événement Présence pour le protocole d'initialisation de session (SIP)

Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé

Le présent document décrit l'utilisation du protocole d'initialisation de session (SIP, *Session Initiation Protocol*) pour les abonnements et les notifications de présence. Présence est défini comme la volonté et la capacité d'un usager à communiquer avec d'autres usagers sur le réseau. Historiquement, la présence a été limitée aux indicateurs "en ligne" et "hors ligne" ; la notion de présence est ici plus large. Les abonnements et notifications de présence sont pris en charge en définissant un paquetage d'événement au sein du cadre général de la notification d'événement SIP. Ce protocole est aussi conforme au cadre du profil commun de présence (CPP, *Common Presence Profile*).

Table des Matières

1. Introduction

Présence, aussi appelé informations de présence, porte la capacité et la volonté d'un usager de communiquer à travers un ensemble d'appareils. La [RFC2778] définit un modèle et une terminologie de description des systèmes qui fournissent des informations de présence. Dans ce modèle, un service de présence est un système qui accepte, mémorise, et distribue les informations de présence aux parties intéressées, appelées des observateurs. Un protocole de présence est un protocole qui fournit un service de présence sur l'Internet ou sur tout réseau IP.

Le présent document propose l'utilisation du protocole d'initialisation de session (SIP) [RFC3261] comme protocole de présence. C'est accompli par une instanciation concrète du cadre général de notification d'événement défini pour SIP [RFC3265], et à ce titre, il fait usage des méthodes SUBSCRIBE et NOTIFY qui y sont définies. Précisément, le présent document définit un paquetage d'événements, comme décrit dans la [RFC3265]. SIP convient particulièrement bien comme protocole de présence. Les services de localisation de SIP contiennent déjà des informations de présence, sous la forme d'enregistrements. De plus, les réseaux SIP sont capables d'acheminer les demandes provenant de tout usager sur le réseau au serveur qui détient l'état d'enregistrement pour un usager. Comme cet état est un composant clé de la présence d'usager, ces réseaux SIP peuvent permettre que les demandes SUBSCRIBE soient acheminées au même serveur. Le présent mémoire signifie que les réseaux SIP peuvent être réutilisés pour établir une connexité globale pour les abonnements et notifications de présence.

Ce paquetage d'événements se fonde sur le concept d'un agent de présence qui est une nouvelle entité logique capable d'accepter les abonnements, de mémoriser l'état d'abonnement, et de générer les notifications lorsque il y a des changements de présence. L'entité est définie comme logique, car elle est généralement corésidente avec une autre entité.

Ce paquetage d'événement est aussi conforme au cadre du profil de présence commun (CPP, *Common Presence Profile*) qui a été défini dans la [RFC3859]. Cela permet à SIP pour présence d'inter fonctionner facilement avec d'autres systèmes de présence conformes à CPP.

2. Terminologie

Dans ce document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP14, [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

3. Définitions

Le présent document utilise les termes comme ils sont définis dans la [RFC2778]. De plus, les termes suivants sont définis et/ou précisés:

Agent d'usager présence (PUA, *Presence User Agent*) : il manipule les informations de présence pour une présentité. Cette manipulation peut être l'effet collatéral de quelque autre action (comme l'envoi d'une demande SIP REGISTER pour ajouter un nouveau contact) ou peut être faite explicitement par la publication de documents de présence. On permet explicitement plusieurs PUA par présentité. Cela signifie qu'un usager peut avoir plusieurs appareils (comme un téléphone cellulaire et un assistant numérique personnel (PDA, *Personal Digital Assistant*)) dont chacun génère indépendamment une composante des informations globales de présence pour une présentité. Les PUA poussent les données dans le système de présence, mais lui sont extérieurs, en ce qu'ils ne reçoivent pas de messages SUBSCRIBE ni n'envoient de messages NOTIFY.

Agent de présence (PA, *Presence Agent*) : c'est un agent d'utilisateur SIP qui est capable de recevoir des demandes SUBSCRIBE, d'y répondre, et de générer les notifications des changements de l'état de présence. Un agent de présence doit avoir connaissance de l'état de présence d'une présentité. Cela signifie qu'il doit avoir accès aux données de présence manipulées par les PUA pour la présentité. Une façon de le faire est de colocaliser le PA avec le mandataire/registraire.

Une autre façon est de le colocaliser avec l'agent d'utilisateur de présence de la présentité. Cependant, ce ne sont pas les seules façons, et la présente spécification ne fait pas de recommandation sur l'endroit où devrait être localisée la fonction de PA. Un PA est toujours adressable avec un URI SIP qui identifie la présentité de façon univoque (c'est-à-dire, sip:joe@example.com). Il peut y avoir plusieurs PA pour une présentité particulière,

chacune d'elle ayant des liens avec un sous-ensemble des abonnements actuellement actifs pour la présentité. Un PA est aussi un notificateur (défini dans la [RFC3265]) qui prend en charge le paquetage d'événements présence.

Serveur de présence : c'est une entité physique qui peut agir comme agent de présence ou comme serveur mandataire pour les demandes SUBSCRIBE. Lorsque il agit comme PA, il connaît les informations de présence de la présentité grâce à des moyens fournis par le protocole. Lorsque il agit comme mandataire, les demandes SUBSCRIBE sont relayées à une autre entité qui peut agir comme un PA.

Serveur bordure de présence : c'est un agent de présence qui est colocalisé avec un PUA. Il connaît les informations de présence de la présentité parce que il est colocalisé avec l'entité qui manipule ces informations de présence.

4. Vue d'ensemble du fonctionnement

Dans cette section, on présente une vue d'ensemble du fonctionnement du paquetage d'événement. Elle décrit le comportement qui est en partie documenté ici, et en partie dans le cadre d'événement SIP [RFC3265], et en partie dans la spécification de SIP [RFC3261], afin de fournir des précisions sur ce paquetage pour les lecteurs qui ne seraient pas entièrement familiarisés avec ces spécifications. Cependant, la sémantique détaillée de ce paquetage exige que le lecteur soit familiarisé avec les événements SIP et la spécification SIP elle-même.

Lorsque une entité, l'abonné, souhaite connaître les informations de présence sur un utilisateur, il crée une demande SUBSCRIBE. Cette demande identifie la présentité désirée dans l'URI de demande, en utilisant un URI SIP, un URI SIPS [RFC3261] ou un URI de présence (pres) [RFC3859]. La demande SUBSCRIBE est portée par les mandataires SIP comme le serait toute autre demande SIP. Dans la plupart des cas, elle arrive finalement à un serveur présence, qui peut soit générer une réponse à la demande (auquel cas il agit comme agent de présence pour la présentité) soit la déléguer à un serveur bordure de présence. Si le serveur bordure de présence traite l'abonnement, il agit comme agent de présence pour la présentité. La décision d'un serveur de présence de mandater ou de terminer la demande SUBSCRIBE est une affaire locale ; cependant, on décrit une façon d'effectuer une telle configuration, en utilisant REGISTER.

L'agent de présence (qu'il soit dans le serveur de présence ou dans le serveur bordure de présence) authentifie d'abord l'abonnement, puis il l'autorise. Les moyens de l'autorisation sortent du domaine d'application du présent protocole, et on pense que de nombreux mécanismes seront utilisés. Si il est autorisé, une réponse 200 OK est retournée. Si l'autorisation n'a pas pu être obtenue cette fois, l'abonnement est considéré comme "en instance", et une réponse 202 est retournée. Dans les deux cas, le PA envoie un message NOTIFY immédiat qui contient l'état de la présentité et de l'abonnement. L'état de la présentité peut être fautif dans le cas d'un abonnement en instance, indiquant, par exemple, quand, même hors ligne, quel est l'état réel de la présentité. Cela est fait pour protéger la confidentialité de la présentité, qui peut ne pas vouloir révéler qu'elle n'a pas fourni l'autorisation à l'abonné. Comme l'état de la présentité change, le PA génère des NOTIFY qui contiennent ces changements d'état à tous les abonnés qui ont des abonnements autorisés. Les changements d'état de l'abonnement lui-même peuvent aussi déclancher des demandes NOTIFY ; cet état est porté dans le champ d'en-tête État de souscription du NOTIFY, et va normalement indiquer si l'abonnement est actif ou en instance.

Le message SUBSCRIBE établit un "dialogue" avec l'agent de présence. Un dialogue est défini dans la [RFC3261], et il représente l'état SIP entre une paire d'entités pour faciliter les échanges de message d'homologue à homologue. Cet état inclut les numéros de séquence pour les messages dans les deux directions (SUBSCRIBE depuis l'abonné, NOTIFY depuis l'agent de présence) en plus d'un ensemble de chemins et d'un URI de cible distante. L'ensemble de chemins est une liste d'URI SIP (ou SIPS) qui identifient les serveurs mandataires SIP qui devront être visités le long du chemin des rafraîchissements de SUBSCRIBE ou des demandes NOTIFY. L'URI de cible distante est l'URI SIP ou SIPS qui identifie la cible du message – l'abonné, dans le cas de NOTIFY, ou l'agent de présence, dans le cas d'un rafraîchissement de SUBSCRIBE.

SIP fournit une procédure appelée enregistrement de chemin qui permet aux serveurs mandataires de demander d'être sur le chemin des messages NOTIFY et des rafraîchissements de SUBSCRIBE. Cela se fait en insérant un URI dans le champ d'en-tête Record-Route dans la demande SUBSCRIBE initiale.

L'abonnement persiste pendant une durée qui est négociée au titre du SUBSCRIBE initial. L'abonné va devoir rafraîchir l'abonnement avant qu'il arrive à expiration, si il souhaite conserver l'abonnement. Cela se fait par l'envoi d'un rafraîchissement SUBSCRIBE au sein du même dialogue qu'établi par le SUBSCRIBE initial. Ce SUBSCRIBE est presque identique à l'initial, mais contient une étiquette dans le champ d'en-tête To, une plus forte valeur de champ d'en-tête CSeq, et éventuellement, un ensemble de valeurs de champ d'en-tête Route qui identifient le chemin des mandataires que va prendre la demande.

L'abonné peut terminer l'abonnement en envoyant un SUBSCRIBE, au sein du dialogue, avec une valeur de champ d'en-tête Expires (qui indique la durée de l'abonnement) de zéro. Cela cause la terminaison immédiate de l'abonnement. Une demande NOTIFY est alors générée par l'agent de présence avec l'état le plus récent. En fait, le comportement de l'agent de présence pour le traitement d'une demande SUBSCRIBE avec Expires à zéro n'est pas différent de celui pour toute autre valeur d'expiration ; les demandes SUBSCRIBE autorisées ou en instance résultent en un déclanchement d'un NOTIFY avec l'état en cours de la présentité et de l'abonnement.

L'agent de présence peut terminer l'abonnement à tout moment. Pour ce faire, il envoie une demande NOTIFY avec un champ d'en-tête État d'abonnement indiquant que l'abonnement est terminé. Un paramètre de cause peut être fourni qui en donne la raison.

Il est aussi possible d'aller chercher l'état de présence en cours, d'où il résulte une notification en une fois qui contient l'état en cours. Cela se fait par l'envoi d'une demande SUBSCRIBE avec une expiration immédiate.

5. Utilisation des URI de présence

Une présentité est identifiée de la façon la plus générale par un URI présence [RFC3859], qui est de la forme pres:usager@domaine. Ces URI sont résolus en URI spécifiques du protocole, comme les URI SIP ou SIPS, par des politiques de transposition spécifiques du domaine tenues par un serveur.

Il est très possible qu'un usager ait à la fois un URI SIP (et/ou SIPS) et un URI pres pour identifier à la fois lui-même et les autres usagers. Cela conduit à des questions sur comment ces URI se relient et lesquels sont à utiliser.

Dans certaines instances, un usager commence avec un format d'URI, comme l'URI pres, et apprend un URI dans un format différent par des moyens tirés du protocole. Par exemple, une demande SUBSCRIBE envoyée à un URI pres va résulter en l'acquisition d'un URI SIP ou SIPS pour la présentité d'après le champ d'en-tête Contact du 200 OK à la demande SUBSCRIBE. Autre exemple, un mécanisme du DNS pourrait être défini qui permettrait une recherche d'URI pres pour obtenir un URI SIP ou SIPS. Au cas où un URI est acquis d'un autre moyen par l'intermédiaire du protocole, ce moyen va souvent fournir une sorte de délimitation qui va limiter la durée de vie de l'URI acquis. Le DNS, par exemple, fournit un TTL qui va limiter la portée de l'URI. Ces portées sont très utiles pour éviter des URI périmés ou en conflit pour identifier la même ressource. Pour s'assurer qu'un usager peut toujours déterminer si un URI acquis est encore valide, il est RECOMMANDÉ que les systèmes qui fournissent des services de recherche d'URI présence aient une sorte de mécanisme de limitation.

Si un abonné a seulement connaissance d'un URI pres indépendant du protocole pour une présentité, il suit les procédures définies dans la [RFC3861]. Ces procédures vont résulter en le placement de l'URI pres dans l'URI de demande de la demande SIP, suivi par l'usage des procédures du DNS définies dans la [RFC3861] pour déterminer l'hôte auquel envoyer la demande SIP. Bien sûr, un mandataire sortant local peut aussi être utilisé, comme spécifié dans la [RFC3261]. Si l'abonné a connaissance des deux URI pres indépendant du protocole et de l'URI SIP ou SIPS pour la même présentité, et si les deux sont valides (comme exposé ci-dessus) il DEVRAIT utiliser le format d'URI pres. Bien sûr, si l'abonné ne connaît que l'URI SIP pour la présentité, cet URI est utilisé, et le traitement standard de la [RFC3261] va avoir lieu. Lorsque on utilise l'URI pres, tous les mandataires le long du chemin de la demande SUBSCRIBE qui ne comprennent pas le schéma d'URI vont rejeter la demande. À ce titre, on pense que de nombreux systèmes seront initialement déployés en ne fournissant aux usagers qu'un URI SIP.

Les messages SUBSCRIBE contiennent aussi des identifiants logiques qui définissent l'origine et le receveur de l'abonnement (les champs d'en-tête To et From). Ces en-têtes peuvent prendre un URI aussi bien pres que SIP. Lorsque l'abonné connaît les deux URI pres et SIP pour sa propre identité, il DEVRAIT utiliser l'URI pres dans l'en-tête From. De même, lorsque l'abonné connaît les deux URI pres et SIP pour la présentité désirée, il DEVRAIT utiliser l'URI pres dans le champ d'en-tête To.

L'usage de l'URI pres au lieu de l'URI SIP au sein du message SIP supporte l'interopérabilité à travers les passerelles avec les autres systèmes conformes à CPP. Il assure une forme indépendante du protocole pour l'identification qui peut être passée entre les systèmes. Sans une telle identité, les passerelles seraient forcées de transposer les URI SIP en format d'adressage des autres protocole. Généralement, cela se fait en convertissant l'URI SIP en la forme <schéma-de-protocole-étranger>:<URI SIP codé>@<passerelle>. Cela est fait couramment dans les systèmes de messagerie électronique, et pose de nombreux problèmes connus. L'usage de l'URI pres est un DEVRAIT, et non un DOIT, pour permettre les cas où il est connu qu'il n'y a pas de passerelle présente, ou lorsque l'usage de l'URI pres va causer des problèmes d'interopérabilité avec des composants SIP qui n'acceptent pas l'URI pres.

Les champs Contact, Record-Route et Route n'identifient pas d'entités logiques, mais plutôt des entités concrètes utilisées

pour la messagerie SIP. SIP [RFC3261] spécifie les règles de leur construction.

6. Paquetage d'événement Présence

Le cadre d'événement SIP [RFC3265] définit une extension à SIP pour l'abonnement à, et la réception, des notifications d'événements. Il laisse la définition de nombreux aspects de ces événements aux extensions concrètes, connues sous le nom de paquetages d'événements. Le présent document est qualifié comme paquetage d'événement. La présente section fournit les informations requises pour tous les paquetages d'événement par la [RFC3265].

6.1 Nom de paquetage

Le nom de ce paquetage est "presence". Comme spécifié dans la [RFC3265], cette valeur apparaît dans le champ d'en-tête Event présent dans les demandes SUBSCRIBE et NOTIFY.

Exemple : Event: presence

6.2 Paramètres de paquetage d'événement

Le cadre d'événement SIP permet que les paquetages d'événement définissent des paramètres supplémentaires portés dans le champ d'en-tête Event. Le présent paquetage, présence, ne définit aucun paramètre supplémentaire.

6.3 Corps SUBSCRIBE

Une demande SUBSCRIBE PEUT contenir un corps. L'objet du corps dépend de son type. Les abonnements ne vont normalement pas contenir de corps.

L'URI de demande, qui identifie la présentité, combiné avec le nom du paquetage d'événement, est suffisant pour présence.

Un type de corps qui peut être inclus dans une demande SUBSCRIBE est un document filtre. Ces filtres demandent que seuls certains événements de présence génèrent des notifications, ou vont demander une restriction sur l'ensemble des données retournées dans les demandes NOTIFY. Par exemple, un filtre de présence pourrait spécifier que les notifications ne devraient être générées que lorsque change l'état de la boîte aux lettres instantanée de l'usager [RFC2778]. Il pourrait aussi dire que le contenu de ces notifications devrait seulement contenir l'état de la boîte aux lettres instantanée. Les documents filtre ne sont pas spécifiés dans le présent document, et au moment de sa rédaction on pense qu'ils feront l'objet d'une activité future de normalisation.

Le respect de ces filtres est à la discrétion de la politique de l'agent de présence.

Si la demande SUBSCRIBE ne contient pas de filtre, cela dit à l'agent de présence qu'il n'y a pas de filtre à appliquer. Le PA DEVRAIT envoyer des demandes NOTIFY à la discrétion de sa propre politique.

6.4 Durée d'abonnement

La présence de l'usager change par suite de nombreux événements. Par exemple :
- o activation et désactivation d'un téléphone cellulaire,
- o modification de l'enregistrement d'un téléphone logiciel,
- o changement de l'état sur un outil de messagerie instantanée.

Ces événements sont normalement déclanchés par une intervention humaine, et surviennent à une fréquence de l'ordre de quelques secondes à quelques heures. À ce titre, les abonnements devraient avoir un temps d'expiration dans le milieu de cette gamme, qui est en gros d'une heure. Donc, le temps d'expiration par défaut pour les abonnements dans ce paquetage est de 3600 secondes. Selon la [RFC3265], l'abonné PEUT spécifier un autre temps d'expiration dans le champ d'en-tête Expires.

6.5 Corps NOTIFY

Comme décrit dans la [RFC3265], le message NOTIFY va contenir des corps qui décrivent l'état de la ressource souscrite. Ce corps est dans un format cité dans le champ d'en-tête Accept de SUBSCRIBE, ou un format par défaut spécifique du paquetage si le champ d'en-tête Accept a été omis dans SUBSCRIBE.

Dans ce paquetage d'événement, le corps de la notification contient un document présence. Ce document décrit la présence de la présentité à laquelle l'abonnement a été souscrit. Tous les abonnés et les notificateurs DOIVENT prendre en charge le format de données de présence "application/pidf+xml" décrit dans la [RFC3863]. La demande d'abonnement PEUT contenir un champ d'en-tête Accept. Si un tel champ d'en-tête n'est pas présent, il a une valeur par défaut de "application/pidf+xml". Si le champ d'en-tête est présent, il DOIT inclure "application/pidf+xml", et PEUT inclure tous autres types capables de représenter la présence de l'usager.

6.6 Notifier le traitement des demandes SUBSCRIBE

Sur la base des procédures d'acheminement par mandataire définies dans la spécification SIP, la demande SUBSCRIBE va arriver à une agent de présence (PA, *presence agent*). Ce paragraphe définit le traitement spécifique du paquetage chez le PA d'une demande SUBSCRIBE. Les règles générales de traitement pour les demandes sont couvertes au paragraphe 8.2 de la [RFC3261], en plus du traitement général de SUBSCRIBE dans la [RFC3265].

La présence de l'usager est une information très sensible. Comme les implications de la divulgation des informations de présence peuvent être sévères, de fortes exigences sont imposées au PA en ce qui concerne le traitement de l'abonnement, en particulier en matière d'authentification et d'autorisation.

6.6.1 Authentification

Un agent de présence DOIT authentifier toutes les demandes d'abonnement. Cette authentification peut être faite en utilisant tout mécanisme défini dans la [RFC3261]. Noter que la mise en œuvre du résumé est obligatoire, comme spécifié dans la RFC3261.

Dans les systèmes à un seul domaine, où les abonnés partagent tous des secrets avec le PA, la combinaison de l'authentification par résumé sur la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC2246] assure une solution sûre et pratique pour l'authentification. Ce cas d'utilisation est décrit au paragraphe 26.3.2.1 de la [RFC3261].

Dans les scénarios inter-domaines, il est plus difficile d'établir une identité authentifiée de l'abonné. On prévoit que l'authentification sera souvent établie à travers une confiance transitive. Les mécanismes SIP pour l'identité attestée par le réseau peuvent être appliqués pour établir l'identité de l'abonné [RFC4474].

Une présentité PEUT choisir de se représenter avec un URI SIPS. Par "se représenter", on veut dire que l'usager représenté par la présentité détient, sur une carte de visite, des pages de la Toile, et ainsi de suite, un URI SIPS pour sa présentité. La sémantique associée à cet URI, comme décrite dans la [RFC3261], exige l'usage de TLS sur chaque bond entre l'abonné et le serveur dans le domaine de l'URI. Cela donne des assurances supplémentaires (mais pas de garantie absolue) que l'identité a été vérifiée à chaque bond.

Un autre mécanisme pour l'authentification est S/MIME. Son usage avec SIP est décrit en détails dans la [RFC3261]. Il fournit un mécanisme d'authentification de bout en bout qui peut être utilisé pour q'un PA établisse l'identité de l'abonné.

6.6.2 Autorisation

Une fois authentifié, le PA prend une décision d'autorisation. Un PA NE DOIT PAS accepter un abonnement si l'autorisation n'a pas été fournie par la présentité. Les moyens par lesquels l'autorisation est fournie sortent du domaine d'application du présent document. L'autorisation peut avoir été fournie longtemps auparavant par des listes d'accès, éventuellement spécifiée sur une page de la Toile. L'autorisation peut avoir été fournie par le téléchargement d'un document contenant une sorte de liste de contrôle d'accès standard. Les serveurs d'autorisation en arrière plan, tels que le serveur DIAMETER [RFC3588], peuvent aussi être utilisés. Il est aussi utile d'être capable d'interroger l'usager sur l'autorisation à la suite de la réception d'une demande d'abonnement pour laquelle aucune information d'autorisation n'a été fournie. Le paquetage de gabarit d'événement "watcherinfo" pour SIP [RFC3857] définit un moyen par lequel une présentité peut apprendre qu'un usager a tenté de s'abonner à elle, de sorte qu'elle peut alors prendre une décision d'autorisation.

Les décisions d'autorisation peuvent être très complexes. En fin de compte, toutes les décisions d'autorisation peuvent être transposées en un de ces trois états : rejeté, réussite, et en cours. Tout abonnement pour lequel le client est autorisé à recevoir des informations sur un sous ensemble d'état de présence à un certain moment est un abonnement réussi. Tout abonnement pour lequel le client ne va jamais recevoir d'information sur un sous ensemble quelconque de l'état de présence est un abonnement rejeté. Tout abonnement pour lequel on ne sait pas encore si il est réussi ou rejeté est en cours. Généralement, un abonnement en cours se produit lorsque le serveur ne peut pas obtenir l'autorisation au moment de l'abonnement, mais peut être capable de le faire un peu plus tard, peut-être lorsque la présentité devient disponible.

Les codes de réponse appropriés pour convoyer un abonnement réussi, rejeté, ou en cours (respectivement, 200, 403 ou 603, et 202) sont décrits dans la [RFC3265].

Si la ressource n'est pas dans un état significatif, la [RFC3265] permet que le corps du NOTIFY initial soit vide. Dans le cas de présence, ce NOTIFY PEUT contenir un document présence. Ce document indiquerait quel état de présence l'abonné est autorisé à voir ; c'est interprété par l'abonné comme l'état de présence actuel de la présentité. Pour les abonnements en instance, l'état de la présentité DEVRAIT inclure une sorte de note textuelle qui indique un état en cours.

Un blocage poli, comme décrit dans la [RFC2779], est possible en générant un 200 OK à l'abonnement même si il a été rejeté (ou marqué en instance). Bien sûr, un NOTIFY immédiat sera quand même envoyé.
Le contenu du document de présence dans un tel NOTIFY est à la discrétion de la mise en œuvre, mais DEVRAIT être construit de telle façon qu'il ne soit pas révélé au candidat abonné dont la demande a en fait été bloquée. Normalement, on fait cela en indiquant "hors ligne" ou un état équivalent pour une seule adresse de contact.

6.7 Génération par le notificateur des demandes NOTIFY

La [RFC3265] détaille le formatage et la structure des messages NOTIFY. Cependant, les paquetages sont obligés de fournir des informations détaillées sur le moment d'envoyer un NOTIFY, comment calculer l'état de la ressource, comment générer des informations d'état neutres ou fausses, et si les informations d'état sont complètes ou partielles. Ce paragraphe décrit ces détails pour le paquetage d'événement présence.

Un PA PEUT envoyer un NOTIFY à tout moment. Normalement, il va en envoyer un lorsque l'état de la présentité change. La demande NOTIFY PEUT contenir un corps qui indique l'état de la présentité. L'heure à laquelle le NOTIFY est envoyé pour un abonné particulier, et le contenu du corps au sein de cette notification, sont soumis à toutes les règles spécifiées par la politique d'autorisation qui gouverne l'abonnement. Le présent protocole ne limite en aucune façon la portée de telles politiques. Au minimum, une politique raisonnable est de générer les notifications lorsque l'état d'une quelconque des parties à présence change. Ces notifications devraient contenir l'état complet et actuel de l'état de présence de la présentité tel que connu de l'agent de présence. De futures extensions pourront être définies pour permettre à un abonné de demander que les notifications ne contiennent que les changements des informations de présence, plutôt que l'état complet.

Dans le cas d'abonnement en instance, lorsque l'autorisation finale est déterminée, un NOTIFY peut être envoyé. Si le résultat d'une décision d'autorisation a été la réussite, un NOTIFY DEVRAIT être envoyé et DEVRAIT contenir un document de présence avec l'état actuel de la présentité. Si l'abonnement est rejeté, un NOTIFY PEUT être envoyé. Comme décrit dans la [RFC3265], le champ d'en-tête Subscription-State indique l'état de l'abonnement.

Le corps du NOTIFY DOIT être envoyé en utilisant un des types énumérés dans le champ d'en-tête Accept dans la plus récente demande SUBSCRIBE, ou en utilisant le type "application/pidf+xml" si aucun champ d'en-tête Accept n'était présent.

Les moyens par lesquels le PA apprend l'état de la présentité sortent aussi du domaine d'application de cette recommandation. Les enregistrements peuvent fournir une composante de l'état de la présentité. Cependant, les moyens par lesquels un PA utilise les enregistrements pour construire un document de présence sont un choix de la mise en œuvre. Si un PUA souhaite informer explicitement l'agent de présence de son état de présence, il devrait publier explicitement le document de présence (ou la partie de celui-ci qui le concerne) plutôt que de tenter de manipuler leurs enregistrements pour réaliser le résultat désiré.

Pour des raisons de confidentialité, il sera fréquemment nécessaire de chiffrer le contenu des notifications. Cela peut être réalisé en utilisant S/MIME. Le chiffrement peut être effectué en utilisant la clé de l'abonné tel qu'identifié dans le champ From de la demande SUBSCRIBE. De même, l'intégrité des notifications est importante pour les abonnés. À ce titre, le contenu des notifications PEUT assurer l'authentification et la protection de l'intégrité du message en utilisant S/MIME. Comme le NOTIFY est généré par le serveur de présence, qui peut ne pas avoir accès à la clé de l'usager représenté par la présentité, il va fréquemment se trouver que le NOTIFY est signé par un tiers. Il est RECOMMANDÉ que la signature soit par une autorité sur le domaine de la présentité. En d'autres termes, pour un usager pres:user@example.com, le signataire du NOTIFY DEVRAIT être l'autorité pour example.com.

6.8 Traitement des demandes NOTIFY par l'abonné

La [RFC3265] laisse aux paquetages d'événements le soin de décrire le processus que suit le souscripteur à réception d'une demande NOTIFY, incluant toute logique requise pour former un état de ressource cohérent.

Dans la présente spécification, chaque NOTIFY contient soit aucun document de présence, soit un document représentant l'état complet et cohérent de la présentité. Au sein d'un dialogue, le document de présence dans la demande NOTIFY qui a

la valeur la plus forte de champ d'en-tête CSeq est celui qui est en cours. Lorsque aucun document n'est présent dans ce NOTIFY, le document de présence présent dans le NOTIFY qui a la plus forte valeur de CSeq est utilisé. Les extensions qui spécifient l'utilisation d'un état partiel pour les présentités vont avoir besoin de dire comment est réalisé un état cohérent.

6.9 Traitement des demandes fourchues

La [RFC3265] exige que chaque paquetage décrive le traitement des demandes SUBSCRIBE fourchées.

La présente spécification ne permet qu'un seul dialogue soit construit par suite de l'émission d'une demande SUBSCRIBE initiale. Cela garantit qu'un seul PA génère les notifications pour une souscription particulière à une certaine présentité. Il résulte de cela qu'une présentité peut avoir plusieurs PA actifs, mais ils devraient être homogènes, de sorte que chacun puisse générer le même ensemble de notifications pour la présentité. La prise en charge de PA hétérogènes, dont chacun génère des notifications pour un sous ensemble de données de présence, est complexe et difficile à gérer. Le faire exigerait que le souscripteur agisse comme agrégateur pour les données de présence. Cette fonction d'agrégation ne peut raisonnablement être effectuée que par des agents représentant la présentité. Donc, si l'agrégation est nécessaire, elle DOIT être faite dans un PA représentant la présentité.

Le paragraphe 4.4.9 de la [RFC3265] décrit le processus requis pour garantir la création d'un seul dialogue en réponse à une demande SUBSCRIBE.

6.10 Taux de notifications

La [RFC3265] exige que chaque paquetage spécifie le taux maximum d'envoi des notifications.

Un PA NE DEVRAIT PAS générer des notifications pour une seule présentité à un taux supérieur à une fois toutes les cinq secondes.

6.11 Agents d'état

La [RFC3265] exige que chaque paquetage prenne en considération le rôle des agents d'état dans le paquetage, et si ils sont utilisés, de spécifier comment sont faites l'authentification et l'autorisation.

Les agents d'état sont au cœur de ce paquetage. Chaque fois que le PA n'est pas colocalisé avec le PUA pour la présentité, le PA agit comme un agent d'état. Il collecte l'état de présence auprès du PUA, et l'agrège dans un document de présence. Comme il peut y avoir plusieurs PUA, un agent d'état centralisé est nécessaire pour effectuer cette agrégation. C'est pourquoi les agents d'état sont fondamentaux pour la présence. Bien sûr, il y a un terme spécifique qui les décrit – un serveur de présence.

6.11.1 Agrégation, authentification, et autorisation

Le moyen par lequel l'agrégation est faite dans l'agent d'état est purement une question de politique. La politique va normalement combiner le désir de la présentité avec les désirs du fournisseur. Le présent document ne restreint en aucune façon l'ensemble des politiques qui peuvent être appliquées.

Cependant, il y a clairement un besoin que l'agent d'état ait accès à l'état de la présentité. Cet état est manipulé par le PUA. Une façon dont l'agent d'état peut obtenir cet état est d'y souscrire. Par suite, si il y a 5 PUA qui manipulent l'état de présence pour une seule présentité, l'agent d'état va générer 5 souscriptions, une à chaque PUA. Pour que ce mécanisme soit efficace, tous les PUA DEVRAIENT être capables d'agir comme PA pour l'état qu'ils manipulent, et qu'ils autorisent les souscriptions qui peuvent être authentifiées comme venant du domaine de la présentité.

L'usage des agents d'état n'altère pas de façon significative la façon dont est faite l'authentification par le PA. Tout mécanisme d'authentification SIP peut être utilisé par un agent d'état. Cependant, l'authentification par résumé va exiger que l'agent d'état connaisse le secret partagé entre la présentité et le souscripteur. Cela va exiger des moyens pour transférer en toute sécurité les secrets partagés de la présentité à l'agent d'état.

L'usage des agents d'état a cependant un impact significatif sur l'autorisation. Comme exposé au paragraphe 6.6, un PA est obligé d'autoriser toutes les souscriptions. Si une politique explicite d'autorisation n'a pas été définie, le PA va devoir interroger l'utilisateur pour avoir cette autorisation. En présence d'un serveur bordure (où le PUA est colocalisé avec le PUA) c'est réalisé de façon triviale. Cependant, lorsque les agents d'état sont utilisés (c'est-à-dire, un serveur de présence) on a besoin d'un moyen pour alerter l'utilisateur du besoin d'une décision d'autorisation. C'est la raison d'être du gabarit de paquetage d'événement watcherinfo [RFC3857]. Tous les agents d'état DEVRAIENT prendre en charge le gabarit de paquetage watcherinfo.

6.11.2 Migration

À l'occasion, il convient que la fonction de PA migre d'un serveur à un autre. Par exemple, pour des raisons d'adaptation, la fonction de PA peut résider dans le serveur de présence lorsque le PUA ne fonctionne pas, mais lorsque le PUA se connecte au réseau, le PA fait migrer les souscriptions chez lui afin de réduire l'état dans le réseau. Le mécanisme pour accomplir la migration est décrit au paragraphe 3.3.5 de la [RFC3265]. Cependant, les paquetages doivent définir dans quelles conditions une telle migration va avoir lieu.

Un PA PEUT choisir de faire migrer les souscriptions à tout moment, par configuration, ou par des moyens dynamiques. La demande REGISTER fournit un moyen dynamique pour qu'un serveur de présence découvre que la fonction peut migrer sur un PUA. Précisément, si un PUA souhaite indiquer qu'il prend en charge la fonction de PA, il DEVRAIT utiliser la spécification de capacités de l'appelé [RFC3840] pour indiquer qu'il prend en charge la méthode de demande SUBSCRIBE et le paquetage d'événements présence. La combinaison de ces deux éléments définit un PA. Bien sûr, un serveur de présence peut toujours tenter une migration sans ses indications explicites. Si il échoue avec un code de réponse 405 ou 489, le serveur va savoir que le PUA ne prend pas en charge la fonction de PA. Dans ce cas, le serveur lui-même va devoir agir comme PA pour cette demande d'abonnement. Une fois qu'un tel échec s'est produit, le serveur NE DEVRAIT PAS tenter d'autre migration sur ce PUA pour la durée de son enregistrement. Cependant, pour éviter le trafic supplémentaire généré par ces échecs de demandes, un serveur de présence DEVRAIT prendre en charge l'extension de capacités de l'appelé.

De plus, l'indication de prise en charge de la demande SUBSCRIBE et du paquetage d'événement présence n'est pas suffisante pour la migration des souscriptions. Un PA NE DEVRAIT PAS faire migrer l'abonnement si il compose des documents de présences agrégés reçus de plusieurs PUA.

7. Découverte de l'état Présence

Les informations de présence peuvent être obtenues de nombreuses façons par le PA. Aucun mécanisme spécifique n'est rendu obligatoire par la présente spécification. Cette section passe en revue certaines des options, à des fins d'information.

7.1 Colocalisation

Lorsque la fonction de PA est colocalisée avec le PUA, la présence est connue directement par le PA.

7.2 REGISTER

Un UA utilise la méthode SIP REGISTER pour informer le réseau SIP de ses adresses de communications en cours (c'est-à-dire, les adresses de contact). Plusieurs UA peuvent enregistrer indépendamment des adresses de contact pour la même adresse d'enregistrement. Cet état d'enregistrement représente une pièce importante des informations globales de présence pour une présentité. C'est une indication d'accessibilité de base pour la communication.

L'usage des informations de REGISTER pour construire la présence n'est possible que si le PA a accès à la base de données d'enregistrements, et peut être informé des changements de cette base de données. Une façon de réaliser cela est de colocaliser le PA avec le registraire.

Les moyens par lesquels un état d'enregistrement est converti en état de présence est une affaire de politique locale, et sort du domaine d'application de la présente spécification. Cependant, quelques lignes directrices générales peuvent être fournies. L'adresse d'enregistrement dans l'enregistrement (le champ d'en-tête To) identifie la présentité. Chaque champ d'en-tête Contact enregistré identifie un point de communications pour cette présentité, qui peut être modelée en utilisant un tuplet. Noter que l'adresse de contact dans le tuplet n'a pas besoin d'être la même que l'adresse de contact enregistrée. Utiliser plutôt une adresse d'enregistrement permet de passer les communications suivantes d'un observateur à travers les mandataires. C'est utile pour le traitement de politique au nom de la présentité et du fournisseur.

Un PUA qui utilise les enregistrements pour manipuler l'état de présence DEVRAIT faire usage de l'extension SIP de capacités de l'appelé [RFC3840]. Cela permet au PUA de fournir au PA de plus riches informations sur lui-même. Par exemple, la présence du paramètre methods qui fait la liste des méthodes "MESSAGE" indique la prise en charge de la messagerie instantanée.

Les valeurs q provenant du champ d'en-tête Contact [RFC3261] peuvent être utilisées pour établir les priorités relatives entre les diverses adresses de communications dans les champs d'en-tête Contact.

L'usage des enregistrements pour obtenir les informations de présence augmente les exigences pour l'authenticité et

l'intégrité des enregistrements. Donc, les demandes REGISTER utilisées par les agents d'utilisateur de présence DOIVENT être authentifiées.

7.3 Chargement des documents Présence

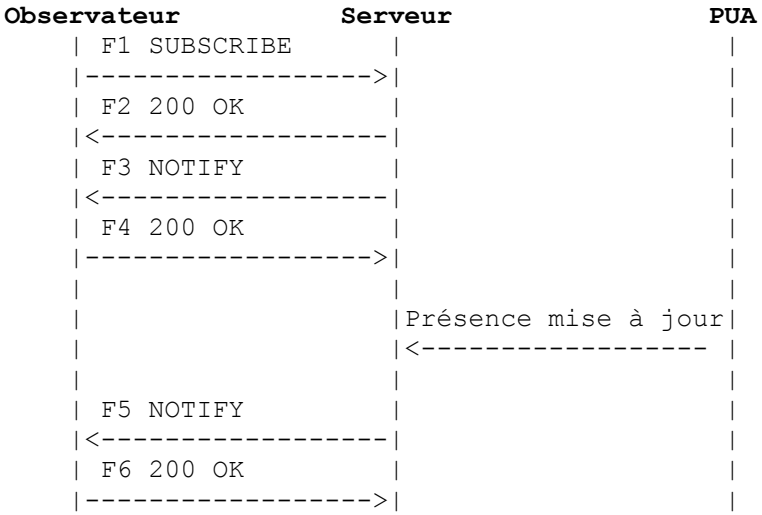
Si il existe un moyen pour télécharge les document de présences du PUA au PA, le PA peut agir comme agrégateur et redistributeur de ces documents. Le PA, dans ce cas, va prendre les documents de présence reçus de chaque PUA pour la même présentité, et fusionner les tuplets à travers tous ces PUA en un seul document de présence. Normalement, cette agrégation va être réalisée par des politiques définies par l'administrateur ou l'utilisateur qui disent comment l'agrégation devrait être faite.

Les moyens spécifiques par lesquels un document de présence est téléchargé à un agent de présence sortent du domaine d'application de la présente spécification. Lorsque un PUA souhaite faire une manipulation directe de la présence qui est distribuée aux abonnés, le téléchargement direct des documents de présence est RECOMMANDÉ.

8. Exemple de flux de messages

Ce flux de messages illustre comment le serveur de présence peut être chargé d'envoyer les notifications pour une présentité. Ce flux suppose que l'observateur a préalablement été autorisé à souscrire à cette ressource chez le serveur.
Dans ce flux, le PUA informe le serveur des informations de présence mises à jour par des moyens non SIP.

Lorsque la valeur du champ d'en-tête Content-Length est "..." cela signifie que la valeur devrait être ce qu'est la longueur calculée du corps.



Détails du message

F1 SUBSCRIBE : observateur --> serveur example.com
SUBSCRIBE sip:resource@example.com SIP/2.0
Via: SIP/2.0/TCP watcherhost.example.com;branch=z9hG4bKnashds7
To: <sip:resource@example.com>
From: <sip:user@example.com>;tag=xfg9
Call-ID: 2010@watcherhost.example.com
CSeq: 17766 SUBSCRIBE
Max-Forwards: 70
Event: presence
Accept: application/pidf+xml
Contact: <sip:user@watcherhost.example.com>
Expires: 600
Content-Length: 0

F2 200 OK serveur example.com --> observateur
SIP/2.0 200 OK
Via: SIP/2.0/TCP watcherhost.example.com;branch=z9hG4bKnashds7

```
    ;received=192.0.2.1
   To: <sip:resource@example.com>;tag=ffd2
   From: <sip:user@example.com>;tag=xfg9
   Call-ID: 2010@watcherhost.example.com
   CSeq: 17766 SUBSCRIBE
   Expires: 600
   Contact: sip:server.example.com
   Content-Length: 0

F3 NOTIFY  serveur example.com -->  observateur
   NOTIFY sip:user@watcherhost.example.com SIP/2.0
   Via: SIP/2.0/TCP server.example.com;branch=z9hG4bKna998sk
   From: <sip:resource@example.com>;tag=ffd2
   To: <sip:user@example.com>;tag=xfg9
   Call-ID: 2010@watcherhost.example.com
   Event: presence
   Subscription-State: active;expires=599
   Max-Forwards: 70
   CSeq: 8775 NOTIFY
   Contact: sip:server.example.com
   Content-Type: application/pidf+xml
   Content-Length: ...
   [Document PIDF]

F4 200 OK observateur --> serveur example.com
   SIP/2.0 200 OK
   Via: SIP/2.0/TCP server.example.com;branch=z9hG4bKna998sk
    ;received=192.0.2.2
   From: <sip:resource@example.com>;tag=ffd2
   To: <sip:user@example.com>;tag=xfg9
   Call-ID: 2010@watcherhost.example.com
   CSeq: 8775 NOTIFY
   Content-Length: 0
F5 NOTIFY serveur example.com --> observateur
   NOTIFY sip:user@watcherhost.example.com SIP/2.0
   Via: SIP/2.0/TCP server.example.com;branch=z9hG4bKna998sl
   From: <sip:resource@example.com>;tag=ffd2
   To: <sip:user@example.com>;tag=xfg9
   Call-ID: 2010@watcherhost.example.com
   CSeq: 8776 NOTIFY
   Event: presence
   Subscription-State: active;expires=543
   Max-Forwards: 70
   Contact: sip:server.example.com
   Content-Type: application/pidf+xml
   Content-Length: ...
   [Nouveau document PIDF]

F6 200 OK
   SIP/2.0 200 OK
   Via: SIP/2.0/TCP server.example.com;branch=z9hG4bKna998sl
    ;received=192.0.2.2
   From: <sip:resource@example.com>;tag=ffd2
   To: <sip:user@example.com>;tag=xfg9
   Call-ID: 2010@watcherhost.example.com
   CSeq: 8776 NOTIFY
   Content-Length: 0
```

9. Considérations pour la sécurité

Il y a de nombreuses considérations de sécurité pour présence. La [RFC2779] mentionne beaucoup d'entre elles, et elles

sont discutées ci-dessus. Cette section les examine une par une.

9.1 Confidentialité

La confidentialité englobe de nombreux aspects d'un système de présence :

- o Les souscripteurs peuvent ne pas vouloir révéler à certains usagers le fait qu'ils sont abonnés ;
- o des usagers peuvent ne pas vouloir révéler qu'ils ont accepté les souscriptions de certains usagers ;
- o les notifications (et les résultats des récupérations) peuvent contenir des données sensibles qui ne devraient pas être révélées à d'autres qu'au souscripteur.

La confidentialité est fournie par une combinaison de chiffrement bond par bond et de chiffrement de bout en bout. Les mécanismes bond par bond fournissent des services de confidentialité adaptables, découragent les attaques qui impliquent l'analyse du trafic, et cachent tous les aspects des messages de présence. Cependant, ils opèrent sur la base de la transitivité de la confiance, et ils causent la révélation du contenu du message aux mandataires. Les mécanismes de bout en bout n'exigent pas la transitivité de la confiance, et ne révèlent les information qu'au receveur désiré. Cependant, le chiffrement de bout en bout ne peut cacher toutes les informations, et est susceptible d'analyse de trafic. Une authentification et un chiffrement forts de bout en bout peuvent être faits en utilisant des clés publiques, et le chiffrement de bout en bout peut être fait en utilisant des clés privées [RFC3211]. Les deux mécanismes bond par bond et de bout en bout vont vraisemblablement être nécessaires pour des services de confidentialité complète.

SIP permet tous les schémas de chiffrement bond par bond, mais la mise en œuvre de TLS est obligatoire pour les serveurs. Donc, il est RECOMMANDÉ que TLS [RFC2246] soit utilisé entre les éléments pour fournir cette fonction. Les détails de l'usage de TLS pour la sécurité de serveur à serveur et de client à serveur sont précisés au paragraphe 26.3.2 de la [RFC3261].

Le chiffrement SIP, utilisant S/MIME, PEUT être utilisé de bout en bout pour la transmission de demandes SUBSCRIBE et NOTIFY.

9.2 Intégrité et authenticité du message

Il est important pour le receveur du message de s'assurer que le contenu du message est réellement ce qui a été envoyé par l'origine, et que le receveur du message soit capable de déterminer qui est réellement l'origine. Cela s'applique aux demandes et réponses de SUBSCRIBE et NOTIFY. Les demandes NOTIFY sont particulièrement importantes. Sans authentification ni protection de l'intégrité, les documents de présences pourraient être falsifiés ou modifiés, trompant l'observateur en lui faisant croire à des informations de présence incorrectes.

La [RFC3261] fournit de nombreux mécanismes pour ces dispositifs. Pour que le PA authentifie l'observateur, il PEUT utiliser le résumé HTTP (Section 22 de la RFC 3261). Par suite, tous les observateurs DOIVENT prendre en charge HTTP Digest. C'est cependant une exigence redondante car tous les agents d'utilisateur SIP sont obligés de le prendre en charge par la RFC 3261. Pour assurer les services d'authenticité et d'intégrité, un observateur PEUT utiliser le schéma SIPS lorsque il souscrit à la présentité. Pour prendre cela en charge, tous les PA DOIVENT prendre en charge TLS et SIPS comme si ils étaient un mandataire (voir le paragraphe 26.3.1 de la RFC 3261).

De plus, SMIME PEUT être utilisé pour l'intégrité et l'authenticité des demandes SUBSCRIBE et NOTIFY. Ceci est décrit à la Section 23 de la RFC 3261.

9.3 Authentification sortante

Lorsque des mandataires locaux sont utilisés pour la transmission de messages sortants, l'authentification du mandataire est RECOMMANDÉE. Ceci est utile pour vérifier l'identité de l'origine, et empêcher l'usurpation d'identité et l'envoi de messages falsifiés sur le réseau d'origine.

9.4 Prévention de la répétition

Des attaques en répétition peuvent être utilisées par un agresseur pour tromper un observateur en lui faisant croire à un état de présence périmé pour une présentité. Par exemple, un document décrivant une présentité comme étant "hors ligne" peut être répété, amenant les observateurs à penser que l'usager n'est jamais en ligne. Cela peut effectivement bloquer les communications avec la présentité.

SIP S/MIME peut assurer l'intégrité et l'authentification des messages sur les corps de demandes SIP. Les observateurs et les PA PEUVENT mettre en œuvre des signatures S/MIME pour empêcher ces attaques en répétition. Lorsque c'est utilisé à

cette fin, le document de présence porté dans la demande NOTIFY DOIT contenir un horodatage. Dans le cas de PIDF, cela est accompli en utilisant l'élément Horodatage, comme décrit à la Section 6 de la [RFC3863]. Les tuplets dont l'horodatage est plus vieux que l'horodatage du plus récent document de présence reçu DEVRAIENT être considérés comme périmés et éliminés.

Finalement, l'authentification par résumé HTTP (qui DOIT être mise en œuvre par les observateurs et les PA) PEUT être utilisée pour empêcher les attaques en répétition, lorsque il y a un secret partagé entre le PA et l'observateur. Dans ce cas, l'observateur peut mettre au défi les demandes NOTIFY avec la qualité de protection auth-int.

9.5 Attaques de déni de service contre les tiers

Les attaques de déni de service (DoS) sont un problème critique pour un protocole de présence ouvert, inter-domaines. Malheureusement, la présence est un bon candidat pour les attaques de DoS réparties (DDOS) à cause de ses propriétés d'amplification. Un seul message SUBSCRIBE pourrait générer un flux presque infini de notifications, tant qu'une source convenablement dynamique de présence peut être trouvée. Donc, une façon simple de lancer une attaque contre une cible est d'envoyer des souscriptions à un grand nombre d'usagers, et dans le champ d'en-tête Contact (qui est là où les notifications sont envoyées) placer l'adresse de la cible. La RFC 3265 fournit des mécanismes pour atténuer ces attaques [RFC3265]. Si un NOTIFY ne reçoit pas d'accusé de réception ou n'a pas été voulu, l'abonnement qui l'a généré est supprimé. Cela élimine les propriétés d'amplification de la fourniture de fausses adresses Contact.

L'authentification et l'autorisation au PA peut aussi empêcher ces attaques. Normalement, la politique d'autorisation ne va pas permettre des abonnements d'observateurs inconnus. Si l'attaque est lancée à partir d'observateurs inconnus de la présentité (un cas courant) les attaques sont contrées.

9.6 Attaques de déni de service contre les serveurs

Les attaques de déni de service peuvent aussi être lancées contre un agent de présence lui-même, afin d'interrompre le service pour une communauté d'usagers. SIP lui-même, avec la [RFC3265], décrit plusieurs mécanismes pour contrer ces attaques.

Un serveur peut empêcher les attaques de style SYN-attack par une prise de contact à quatre phases utilisant une authentification par résumé [RFC3261]. Même si le serveur n'a pas de secret partagé avec le client, il peut vérifier l'adresse IP de source de la demande en utilisant le mécanisme d'utilisateur "anonyme" décrit au paragraphe 22.1 de la [RFC3261]. SIP permet aussi à un serveur de donner pour instruction à un client de retarder l'envoi de sa demande, en utilisant les code de réponse 503 (paragraphe 21.5.4 de la [RFC3261]). Cela peut être utilisé pour détourner des flux de demandes SUBSCRIBE lancées par suite d'une attaque de déni de service répartie.

10. Considérations relatives à l'IANA

La présente spécification enregistre un paquetage d'événement, fondé sur les procédures d'enregistrement définies dans la [RFC3265]. Les informations requises pour un tel enregistrement sont les suivantes :

Nom du paquetage : presence
Paquetage ou gabarit de paquetage : c'est un paquetage.
Document publié : RFC 3856
Personne à contacter : Jonathan Rosenberg, jdrosen@jdrosen.net.

11. Contributeurs

Les individus suivants font partie de l'équipe initiale qui a travaillé à la conception technique de cette spécification:

Jonathan Lennox
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027-7003
mél : lennox@cs.columbia.edu

Robert Sparks
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, Texas 75024
mél : rsparks@dynamicsoft.com

Dean Willis
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, Texas 75024
mél : dwillis@dynamicsoft.com

Henning Schulzrinne
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027-7003
mél : schulzrinne@cs.columbia.edu

Christian Huitema
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
mél : huitema@microsoft.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
mél : bernarda@microsoft.com

David Oran
Cisco Systems
170 West Tasman Dr.
San Jose, CA 95134
mél : oran@cisco.com

David Gurle
Reuters Corporation
mél : David.Gurle@reuters.com

Ben Campbell
mél : ben@nostrum.com

12. Remerciements

Merci à Rick Workman, Adam Roach, Sean Olson, Billy Biggs, Stuart Barkley, Mauricio Arango, Richard Shockey, Jorgen Bjorkner, Henry Sinnreich, Ronald Akers, Paul Kyzivat, Ya-Ching Tan, Patrik Faltstrom, Allison Mankin et Hisham Khartabil pour leurs commentaires et leur soutien à cette spécification.

13. Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393, RFC6665))

[RFC3265] A.B. Roach, "Notification d'événement spécifique du protocole d'initialisation de session (SIP)", juin 2002. (*MàJ par* RFC6446) (*Remplacée par la* RFC6665)

[RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "Indication des capacités d'agent d'utilisateur dans le protocole d'initialisation de session (SIP)", août 2004.

[RFC3857] J. Rosenberg, "Paquetage-gabarit d'événement d'information d'observateur pour le protocole d'initialisation de session (SIP)", août 2004. *(P.S.)*

[RFC3859] J. Peterson, "Profil commun pour les services de présence (CPP)", août 2004. *(P.S.)*

[RFC3861] J. Peterson, "Résolution d'adresse pour la messagerie instantanée et les services de présence", août 2004. *(P.S.)*

[RFC3863] H. Sugano et autres, "Format des données d'information de présence (PIDF)", août 2004.

14. Références pour information

[RFC2778] M. Day, J. Rosenberg et H. Sugano, "Modèle pour Presence et la messagerie instantanée", février 2000.

[RFC2779] M. Day et autres, "Exigences des protocoles Messagerie instantanée / Presence", février 2000. *(Information)*

[RFC3211] P. Gutmann, "Chiffrement fondé sur le mot de passe0pour CMS", décembre 2001. (*Obsolète, voir* RFC3370) *(P.S.)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Obsolète, voir* RFC6733) *(P.S.)*

[RFC4474] J. Peterson et C. Jennings, "Améliorations de la gestion d'identité authentifiée dans le protocole d'initialisation de session (SIP)", août 2006. *(P.S.)*

15. Adresse de l'auteur

Jonathan Rosenberg
dynamicsoft
600 Lanidex Plaza
Parsippany, NJ 07054
USA
mél : jdrosen@dynamicsoft.com

16. Déclaration complète de droits de reproduction

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