Groupe de travail Réseau
Request for Comments : 2779
Catégorie : Information

Traduction Claude Brière de L'Isle

M. Day, Lotus
S. Aggarwal, Microsoft
G. Mohr, Activerse
J. Vincent, Into Networks
février 2000

Exigences des protocoles Messagerie instantanée / Présence

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Il ne spécifie aucune forme de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Présence et messagerie instantanée ont récemment émergé comme nouveau support de communications sur l'Internet. Présence est un moyen pour trouver, restituer et souscrire aux changements des informations de présence (par exemple "en ligne" ou "hors ligne") des autres utilisateurs. La messagerie instantanée est un moyen pour envoyer de petits messages simples qui sont livrés immédiatement aux usagers qui sont en ligne.

Les applications de présence et de la messagerie instantanée utilisent actuellement des protocoles indépendants, non normalisés et non interopérables, développés par divers fabricants. Le but du groupe de travail Protocole de messagerie instantanée et de présence (IMPP, *Instant Messaging et Presence Protocol*) est de définir un protocole standard afin que des applications de messagerie instantanée et/ou de présence, développées en toute indépendance, puissent interopérer à travers l'Internet. Le présent document définit un ensemble minimal d'exigences que doivent satisfaire les IMPP.

Table des matières

1. Terminologie

Les termes suivants sont définis dans la [RFC2778] et sont utilisés avec ces définitions dans le présent document :

Boîte aux Lettres Instantanée
État
Fermé
Informations de Présence
Interrogateur
Mandataire
Message Instantané
Notification
Observateur
Ouvert
Présentité
Principal
Ramasseur
Règles d'Accès
Serveur
Service Présence
Souscripteur
Souscription

Les termes DOIT et DEVRAIT sont utilisés avec le sens suivant lorsque ils spécifient des exigences :

DOIT : Une solution proposée devra satisfaire à cette exigence.
DEVRAIT: Une solution proposée peut choisir de ne pas satisfaire à cette exigence.

Noter que cet usage de DOIT et DEVRAIT diffère de celui de la [RFC2119].

De plus, les termes suivants sont utilisés dans le présent document et définis ici :

Administrateur : C'est un Principal qui a autorité sur un ordinateur et des ressources réseaux locaux, qui gère des domaines ou pare-feu locaux. Pour les besoins de sécurité et autres, un Administrateur a souvent besoin ou veut imposer des restrictions sur l'usage du réseau sur la base du type de trafic, du volume, ou des points d'extrémité. L'Administrateur d'un Principal a autorité sur certains ou tous les ordinateurs et ressources réseau de ce Principal.

Domaine : C'est une portion d'un Espace de Noms.

Entité : C'est une Présentité, un Souscripteur, un Ramasseur, un Interrogateur, ou un Observateur (tous définis dans la [RFC2778]).

Pare-feu : C'est un point de contrôle administratif sur la connexité. Selon les politiques qui sont mises en application, les parties peuvent avoir besoin de prendre des mesures extraordinaires pour établir les communications à travers le Pare-feu.

Identifiant : C'est un moyen d'indiquer un point de contact, destiné à une utilisation publique tel qu'une carte professionnelle. Les numéros de téléphone, les adresses de messagerie électronique, et les URL normaux de page d'accueil sont tous des exemples d'Identifiants dans d'autres systèmes. Les adresses IP numériques, telles que 10.0.0.26, ne le sont pas, ni les URL qui contiennent de nombreux paramètres d'interface de passerelle commune (CGI, *common gateway interface*) ou des identifiants de longueur arbitraire.

Receveur Prévu : C'est le Principal auquel l'envoyeur d'un Message Instantané l'envoie.

Espace de Noms : C'est le système qui transpose du nom d'une Entité en la mise en œuvre concrète de cette Entité. Un Espace de Noms peut être composé d'un certain nombre de Domaines distincts.

Hors Contact : Une situation dans laquelle une Entité et le Service Présence ne peuvent pas communiquer.

Livraison Réussie : Situation dans laquelle un Message Instantané a été transmis à une Boîte aux Lettres Instantanée pour le Receveur Prévu, et la Boîte aux Lettres Instantanée en accuse réception. La Livraison Réussie implique habituellement aussi qu'un Agent d'Utilisateur de Boîte aux Lettres a traité le message de la façon choisie par le Principal. Cependant, La Livraison Réussie n'implique pas que le message a été réellement vu par ce Principal.

2. Exigences partagées

Cette section décrit les exigences autres que de sécurité qui sont communes aux deux services de Présence et de Message Instantané. La Section 6 décrit les exigences spécifiques d'un Service Présence, alors que la Section 7 décrit les exigences spécifiques d'un Service de Message Instantané. La Section 8 décrit les considérations pour la sécurité. Le lecteur notera que la Section 11 est un appendice qui donne le contexte historique et aide à retracer les origines des exigences de la Section 8. La Section 11 n'est cependant pas un état des exigences IMPP actuelles.

Il est prévu que les services de Présence et de Messagerie Instantanée soient particulièrement précieux pour les utilisateurs d'appareils mobiles à accès IP sans fil. Bien sûr, il est prévu que le nombre d'appareils connectés à l'Internet via des moyens sans fil va croître substantiellement dans les années à venir. Il n'est pas raisonnable de penser que des protocoles distincts seront disponibles pour les portions sans fil de l'Internet. De plus, on note que l'infrastructure sans fil mûrit rapidement ; les travaux entrepris par ce groupe devraient prendre en compte l'état de maturité attendu de la technologie dans le calendrier de développement des protocoles Présence et Messagerie Instantanée.

À cette fin, les protocoles conçus par le présent groupe de travail doivent convenir à un fonctionnement dans un contexte normalement associé à des appareils mobiles à accès sans fil, à savoir, latence élevée, faible bande passante et éventuellement connexité intermittente (ce qui conduit au désir de minimiser les délais d'aller-retour) une puissance de calcul modeste, des contraintes de batterie, une petite surface d'affichage, etc. En particulier, les protocoles doivent être conçus pour être raisonnablement efficaces pour de petites charges utiles.

2.1 Espace de noms et administration

2.1.1 Les protocoles DOIVENT permettre qu'un Service Présence soit disponible sans considération de la disponibilité d'un Service Message Instantané, et vice-versa.

2.1.2 Les protocoles ne doivent pas supposer qu'une Boîte aux Lettres Instantanée est nécessairement accessible par le même Identifiant que celui d'une Présentité. Précisément, les protocoles doivent supposer qu'une Boîte aux Lettres Instantanée peut n'avoir pas de Présentité associée, et vice versa.

2.1.3 Les protocoles DOIVENT aussi permettre qu'on accède à une Boîte aux Lettres Instantanée via le même Identifiant que celui d'une certaine Présentité.

2.1.4 L'administration et la désignation des Entités au sein d'un certain Domaine DOIVENT être capables de fonctionner indépendamment des actions dans tout autre Domaine.

2.1.5 Le protocole DOIT permettre un nombre arbitraire de Domaines au sein de l'Espace de Noms.

2.2 Adaptabilité

2.2.1 Il DOIT être possible aux Entités dans un Domaine d'interopérer avec les Entités dans un autre Domaine, sans que les Domaines aient été préalablement présentés l'un à l'autre.

Le protocole DOIT être capable de satisfaire à ses autres exigences fonctionnelles et de performance même lorsque :
-- (**2.2.2**) il y a des millions d'Entités au sein d'un seul Domaine ;
-- (**2.2.3**) il y a des millions de Domaines au sein du seul Espace de Noms ;
-- (**2.2.4**) chaque Souscripteur individuel a des Souscriptions à des centaines de Présentités ;
-- (**2.2.5**) des centaines de Souscripteurs distincts ont des Souscriptions à une seule Présentité ;
-- (**2.2.6**) chaque simple Souscripteur a des Souscriptions aux Présentités dans des centaines de Domaines distincts.
Ce sont des objectifs de conception de protocole dont les mises en œuvre peuvent choisir de baisser les limites.

2.3 Contrôle d'accès

Le Principal qui contrôle une Présentité DOIT être capable de contrôler :
-- (**2.3.1**) quels Observateurs peuvent observer les Informations de Présence de cette Présentité ;
-- (**2.3.2**) quels Observateurs peuvent avoir des Souscriptions aux Informations de Présence de cette Présentité ;
-- (**2.3.3**) quelles Informations de Présence un Observateur particulier va voir pour cette Présentité, sans considérer si l'Observateur les obtient en allant les chercher ou par Notification ;
-- (**2.3.4**) quels autres Principaux, s'il en est, peuvent mettre à jour les Informations de Présence de cette Présentité.

Le Principal qui contrôle une Boîte aux Lettres Instantanée DOIT être capable de contrôler :
-- (**2.3.5**) quels autres Principaux, s'il en est, peuvent envoyer des Messages Instantanés à cette Boîte aux Lettres Instantanée ;
-- (**2.3.6**) quels autres Principaux, s'il en est, peuvent lire les Messages Instantanés de cette Boîte aux Lettres Instantanée.

2.3.7 Le contrôle d'accès DOIT être indépendant de la présence : le Service Présence DOIT être capable de prendre des décisions de contrôle d'accès même lorsque la Présentité est Hors Contact.

2.4 Topologie du réseau

Noter que les intermédiaires tels que les Mandataires peuvent être nécessaires entre les réseaux IP et non IP, et par suite du désir des utilisateurs finaux de fournir l'anonymat et de cacher leur adresse IP.

2.4.1 Le protocole DOIT permettre la création d'une Souscription aussi bien directement que via des intermédiaires, tels que des Mandataires.

2.4.2 Le protocole DOIT permettre l'envoi d'une Notification aussi bien directement que via des intermédiaires, tels que des Mandataires.

2.4.3 Le protocole DOIT permettre l'envoi d'un Message Instantané aussi bien directement que via des intermédiaires, tels que des Mandataires.

2.4.4 Les facilités de mandataire du protocole et les pratiques de transport DOIVENT permettre aux Administrateurs des façons d'activer et de désactiver l'activité du protocole au travers des Pare-feu existants et couramment déployés. Le protocole DOIT spécifier comment il peut effectivement filtrer par de tels Pare-feu.

2.5 Chiffrement et authentification de message

2.5.1 Le protocole DOIT fournir des moyens d'assurer la confiance qu'un message reçu (Notification ou Message Instantané) n'a pas été corrompu ou altéré.

2.5.2 Le protocole DOIT fournir des moyens d'assurer la confiance qu'un message reçu (Notification ou Message Instantané) n'a pas été enregistré et répété par un adversaire.

2.5.3 Le protocole DOIT fournir des moyens d'assurer la confiance qu'un message reçu (Notification ou Message Instantané) n'est lisible que par les Entités que l'envoyeur permet.

2.5.4 Le protocole DOIT permettre à tout client d'utiliser les moyens de s'assurer de la non corruption, de la non répétition, et de la confidentialité, mais le protocole NE DOIT PAS exiger que tous les clients utilisent ces moyens tout le temps.

3. Exigences supplémentaires pour les Informations de Présence

Les exigences de la section 6 ne sont applicables qu'aux Informations de Présence et non aux Messages Instantanés. Les contraintes supplémentaires sur les Informations de Présence dans un système qui prend en charge les Messages Instantanés apparaissent au paragraphe 7.4.

3.1 Format de Présence commun

3.1.1 Toutes les Entités DOIVENT produire et consommer au moins un format de base commun pour les Informations de Présence.

3.1.2 Le format de présence commun DOIT inclure un moyen d'identifier de façon univoque la Présentité dont les Informations de Présence sont rapportées.

3.1.3 Le format de présence commun DOIT inclure un moyen d'encapsuler les informations de contact pour le Principal de la Présentité (si c'est applicable) comme une adresse de messagerie électronique, un numéro de téléphone, une adresse postale, ou équivalent.

3.1.4 Il DOIT y avoir un moyen d'étendre le format commun de présence pour représenter des informations

supplémentaires non incluses dans le format commun, sans léser ou rendre invalides les champs du format commun.

3.1.5 Le groupe de travail doit définir les mécanismes d'extension et d'enregistrement du schéma des informations de présence, y compris des nouvelles conditions d'État et de nouvelles formes pour les Autres Balises de Présence.

3.1.6 Le format de présence DEVRAIT être fondé si possible sur les normes de l'IETF, telles que vCard [RFC2426].

3.2 Recherche et notification de Présence

3.2.1 Un Ramasseur DOIT être capable d'aller chercher des Informations de Présence d'une Présentité même lorsque la Présentité est Hors Contact.

3.2.2 Un Souscripteur DOIT être capable de demander une Souscription aux Informations de Présence d'une Présentité, même lorsque la Présentité est Hors Contact.

3.2.3 Si le Service Présence a des Souscriptions pour les Informations de Présence d'une Présentité, et si ces Informations de Présence changent, le Service Présence DOIT délivrer une Notification à chaque Souscripteur, sauf si il en est empêché par les Règles d'Accès de la Présentité.

3.2.4 Le protocole DOIT fournir un mécanisme pour détecter quand une Présentité ou Souscripteur est passé Hors Contact.

3.2.5 Le protocole NE DOIT PAS compter qu'une Présentité ou Souscripteur lui dise volontairement que le service ne va plus assurer la communication, car une Présentité ou Souscripteur peut se trouver Hors Contact à cause de défaillances inattendues.

3.3 Mise en antémémoire et duplication de Présence

3.3.1 Le protocole DOIT inclure des mécanismes pour autoriser la mise en antémémoire des Informations de Présence.

3.3.2 Le protocole DOIT inclure des mécanismes pour autoriser la mise en antémémoire des Informations de Présence lorsque la copie maîtresse change.

3.3.3 La facilité de mise en antémémoire du protocole NE DOIT PAS contrevenir aux Règles d'accès établies ou restreindre le choix des mécanismes d'authentification/chiffrement.

3.4 Performances

3.4.1 Lorsque une Présentité change ses Informations de Présence, tout Souscripteur à ces informations DOIT recevoir rapidement notification des informations changées, sauf lorsque une telle notification est entièrement empêchée par les Règles d'accès. Cette exigence est satisfaite si chaque Notification de Souscripteur est transportée aussi rapidement qu'un Message Instantané serait transporté à une Boîte aux Lettres Instantanée.

4. Exigences supplémentaires pour les Messages Instantanés

Les exigences de la section 4 ne sont applicables qu'aux Messages Instantanés et non aux Informations de Présence, à l'exception du paragraphe 4.4. Le paragraphe 4.4 décrit les contraintes sur les Informations de Présence qui ne sont pertinentes que pour les systèmes qui prennent en charge à la fois les Messages Instantanés et les Informations de Présence.

4.1 Format commun de message

4.1.1 Toutes les Entités qui envoient et reçoivent des Messages Instantanés DOIVENT mettre en œuvre au moins un format de base commun pour les Messages Instantanés.

4.1.2 Le format de base commun pour un Message Instantané DOIT identifier l'envoyeur et le receveur prévu.

4.1.3 Le format de base commun DOIT inclure une adresse de retour pour que le receveur réponde à l'envoyeur avec un autre Message Instantané.

4.1.4 Le format de base commun DEVRAIT inclure des formes standard d'adresses ou de moyens de contact pour des

supports autres que le Message Instantané, tels que le numéro de téléphone ou l'adresse de messagerie électronique.

4.1.5 Le format de base commun DOIT permettre le codage et l'identification de la charge utile du message afin d'autoriser un contenu non ASCII ou chiffré.

4.1.6 Le protocole doit refléter les bonnes pratiques courantes qui se rapportent à l'internationalisation.

4.1.7 Le protocole doit refléter les bonnes pratiques courantes qui se rapportent à l'accessibilité.

4.1.8 Le groupe de travail DOIT définir les mécanismes d'extension et d'enregistrement du format de message, y compris de nouveaux champs et de nouveaux schémas d'adresse de Boîte aux Lettres Instantanée.

4.1.9 Le groupe de travail DOIT déterminer si le format de message commun inclut des champs pour numéroter ou identifier les messages. Si il y a de tels champs, le groupe de travail DOIT définir la portée dans laquelle de tels identifiants sont uniques et les moyens acceptables pour la génération de tels identifiants.

4.1.10 Le format de base commun DEVRAIT se fonder sur la norme MIME [RFC 2045] de l'IETF.

4.2 Fiabilité

4.2.1 Le protocole DOIT inclure des mécanismes tels qu'un envoyeur puisse être informé de la Livraison Réussie d'un Message Instantané, ou des raisons de son échec. Le groupe de travail doit déterminer quels mécanismes s'appliquent lorsque l'état final de livraison est inconnu, comme par exemple lorsque un message est relayé à des systèmes non IMPP.

4.3 Performances

4.3.1 Le transport de Messages Instantanés DOIT être suffisamment rapide pour permettre des échanges confortables de conversations de courts messages.

4.4 Format de Présence

4.4.1 Le format de présence commun DOIT définir un schéma minimum standard de présence convenable pour le Service de Message Instantané.

4.4.2 Lorsque il est utilisé dans un système qui prend en charge les Messages Instantanés, le format de présence commun DOIT inclure un moyen de représenter les conditions d'état Ouvert et Fermé.

4.4.3 Les conditions d'état Ouvert et Fermé peuvent aussi être appliquées aux modes d'échange de messagerie ou de communication autres que le Service Message Instantanés.

5. Considérations pour la sécurité

Les considérations de sécurité sont traitées au paragraphe 2.3, Contrôle d'accès, et au paragraphe 2.5, Authentification et chiffrement de message.

La présente section décrit plus avant les exigences qui se rapportent à la sécurité que doit satisfaire le protocole.

Les exigences de sécurité sont déduites d'un ensemble "d'attentes de sécurité" générales dont les aspects pratiques et de mise en œuvre ont été évalués et traduits en exigences. Dans l'appendice, on décrit les attentes et le processus utilisé pour les transformer en exigences. Dans la présente section, on énumère simplement l'ensemble consolidé d'exigences dérivées.

Noter que dans les exigences, les Administrateurs peuvent avoir des privilèges qui vont au delà de ceux admis pour les Principaux visés dans ces exigences. (Sauf mention contraire, les attentes individuelles se réfèrent spécifiquement au Principal.) Il revient à chaque mise en œuvre de contrôler l'accès administratif et de mettre en œuvre les privilèges de sécurité des Administrateurs sans compromettre les exigences qui pèsent sur les Principaux.

Sauf notation contraire, A,B,C sont tous des noms de Principaux non Administrateur.

5.1 Exigences en rapport avec les Souscriptions

Lorsque A établit une Souscription pour les Informations de Présence de B :

5.1.1 Le protocole DOIT fournir à A les moyens d'identifier et d'authentifier que la Présentité souscrite est contrôlée par B.

5.1.2 Si A fait ce choix, le protocole NE DEVRAIT PAS rendre la Souscription de A à B visible à un tiers C.

5.1.3 Le protocole DOIT fournir à B les moyens de permettre à A une souscription non authentifiée.

5.1.4 Le protocole DOIT fournir à A les moyens de vérifier la réception précise du contenu que B a choisi de divulguer à A.

5.1.5 B DOIT informer A si B refuse la Souscription de A. Noter que B peut choisir d'accepter la Souscription de A, mais échouer à lui livrer aucune information (c'est ce qu'on appelle un "blocage poli"). Voir le paragraphe 5.1.15.

5.1.6 Le protocole NE DOIT PAS laisser un tiers C forcer A à souscrire aux Informations de Présence sans le consentement de A.

5.1.7 A DOIT être capable d'annuler sa Souscription aux Informations de Présence de B à tout moment et pour une raison quelconque. Lorsque A le fait, le Service Présence arrête d'informer A des changements des Informations de Présence de B.

5.1.8 Le protocole NE DOIT PAS laisser un tiers C non autorisé annuler la Souscription de A à B.

5.1.9 Si la Souscription de A à B est annulée, le service DEVRAIT informer A de cette annulation.

5.1.10 A DEVRAIT être capable de déterminer l'état de la Souscription de A à B, à tout moment.

5.1.11 Le protocole DOIT fournir à B les moyens d'apprendre la Souscription de A à B, aussi bien au moment de l'établissement de la Souscription et qu'après coup.

5.1.12 Le protocole DOIT fournir à B les moyens d'identifier et d'authentifier le Principal, A, du Souscripteur.

5.1.13 Il DOIT être possible à B d'empêcher un Principal donné de souscrire.

5.1.14 Il DOIT être possible à B d'empêcher des Principaux anonymes de souscrire.

5.1.15 Il DOIT être possible à B de configurer le Service Présence de façon à refuser la souscription de A tout en apparaissant à A comme si la souscription avait été accordée (ceci est parfois appelé le "blocage poli"). Le protocole NE DOIT PAS rendre obligatoire au Service Présence de servir des souscriptions qui sont traitées de cette manière.

5.1.16 B DOIT être capable d'annuler à volonté la souscription de A.

5.1.17 Le protocole NE DOIT PAS exiger de A qu'il révèle l'adresse IP de A à B.

5.1.18 Le protocole NE DOIT PAS exiger de B qu'il révèle l'adresse IP de B à A.

5.2 Exigences en rapport avec Notification

Lorsque un Principal B publie les Informations de Présence pour une Notification à un autre Principal A :

5.2.1 Le protocole DOIT fournir les moyens de s'assurer que seul le Principal A auquel B envoie la Notification peut lire la Notification.

5.2.2 A devrait recevoir toutes les Notifications qui lui sont destinées.

5.2.3 Il DOIT être possible à B d'empêcher A de recevoir des notifications, même si il est ordinairement permis à A de voir de telles notifications. Il DOIT être possible à B, si tel est son choix, de notifier différemment à des souscripteurs différents, par des mécanismes de notification différents ou en publiant des contenus différents. Ceci est une variante du "blocage poli".

5.2.4 Le protocole DOIT fournir les moyens de protéger B de la surveillance par un autre Principal C des messages de notification concernant B.

5.2.5 Le protocole NE DOIT PAS exiger que A révèle l'adresse IP de A à B.

5.2.6 Le protocole NE DOIT PAS exiger que B révèle l'adresse IP de B à A.

5.3 Exigences en rapport avec la réception d'une Notification

Lorsque un Principal A reçoit un message notification de la part d'un autre principal B, convoyant des Informations de Présence,

5.3.1 le protocole DOIT fournir à A les moyens de vérifier que les informations de présence sont précisément telles qu'envoyées par B.

5.3.2 Le protocole DOIT s'assurer que seules des entités auxquelles A a souscrit lui envoient des Notifications.

5.3.3 Le protocole DOIT fournir à A les moyens de vérifier que la notification a été envoyée par B.

5.4 Exigences en rapport avec les Messages Instantanés

Lorsque un utilisateur A envoie un Message Instantané M à un autre utilisateur B,

5.4.1 A DOIT recevoir une confirmation de la non livraison.

5.4.2 Si M est livré, B DOIT recevoir le message une seule fois.

5.4.3 Le protocole DOIT fournir à B les moyens de vérifier que A a envoyé le message.

5.4.4 B DOIT être capable de répondre au message via un autre message instantané.

5.4.5 Le protocole NE DOIT PAS toujours exiger que A révèle l'adresse IP de A, pour que A envoie un message instantané.

5.4.6 Le protocole DOIT fournir à A les moyens de s'assurer qu'un autre Principal C ne peut pas voir le contenu de M.

5.4.7 Le protocole DOIT fournir à A les moyens de s'assurer qu'un autre Principal C ne peut pas altérer M, et à B les moyens de vérifier qu'aucune altération n'est survenue.

5.4.8 B doit être capable de lire M.

5.4.9 Le protocole DOIT permettre à A de signer le message, en utilisant les normes existantes pour les signatures numériques.

5.4.10 B DOIT être capable d'empêcher A de lui envoyer des messages.

6. Références

[RFC2778] M. Day, J. Rosenberg et H. Sugano, "Modèle pour Présence et la messagerie instantanée", février 2000. *(Info)*

[RFC2426] F. Dawson, T. Howes, "Profil de répertoire MIME vCard", septembre 1998. *(P.S.)*

[RFC2045] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 1 : Format des corps de message Internet", novembre 1996. *(D. S., MàJ par 2184, 2231, 5335.)*

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

7. Adresse des auteurs

Mark Day
SightPath, Inc.
135 Beaver Street
Waltham, MA 02452
USA
mél : mday@alum.mit.edu

Sonu Aggarwal
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
mél : sonuag@microsoft.com

Jesse Vincent
Into Networks, Inc.
150 Cambridgepark Drive
Cambridge, MA 02140
USA
mél : jesse@intonet.com

Gordon Mohr
mél : gojomo@usa.net

8. Appendice : Attentes de sécurité et exigences dérivées

Le présent appendice se fonde sur les attentes de sécurité exposées sur la liste de discussion de l'impp et rassemblées par Jesse Vincent. La forme originale de numérotation a été préservée dans cet appendice (de sorte qu'il y a plusieurs éléments différents qui sont marqués B1, par exemple). Les exigences dérivées ont de nouveaux numéros qui sont cohérents avec ceux du corps principal du document. Cet appendice est fourni pour assurer la connexion entre les discussions de la liste et les exigences de la Section 8, mais n'est destiné à introduire aucune nouvelle exigence allant au delà de celles présentées des Sections 5 à 8.

8.1 Informations de Présence

Dans le cas d'Informations de Présence, les intérêts de contrôle de la confidentialité du Principal sont primordiaux ; on s'accorde à dire que le "blocage poli" (le refus sans dire que la souscription est refusée, ou en fournissant de fausses informations) devrait être possible.

8.1.1 Souscription

Lorsque l'utilisateur Alice souscrit aux informations de présence d'une autre personne, Bob, Alice s'attend à ce que :

A1. Le Principal B de la Présentité est identifiable et authentifié.
Discussion : Posé comme une exigence. Noter que le protocole devrait fournir à Alice la capacité d'authentification, sans exiger qu'Alice authentifie chaque Souscription. Cet avertissement est rendu nécessaire par les soucis de performances, entre autres, et s'applique à de nombreuses autres exigences déduites ci-dessous. [Exigence 5.1.1]

A2. Aucun tiers ne saura que A a souscrit à B.
Discussion : Il est assez peu raisonnable de la mettre en application telle quelle. Par exemple, dans certaines topologies, rien ne peut empêcher quelqu'un de faire de l'analyse du trafic pour déduire que A a souscrit à B. On devrait simplement exiger que le protocole n'expose pas les informations de souscription de façon évidente. [Exigence 5.1.2]

A3. A a la capacité de souscrire à la présence de B à l'insu de B, si B permet les souscriptions anonymes.
Discussion : Une souscription "anonyme" peut avoir deux implications - (i) B peut permettre une souscription non authentifiée de A, et (ii) B peut n'être pas au courant de l'identité déclarée par A. L'exigence (i) est raisonnable [Exigence 8.1.3], mais (ii) ne paraît pas être une exigence primordiale – cela peut être adéquatement simulé via un pseudonyme de souscription.

A4. A va précisément recevoir ce que B choisit de divulguer à A en ce qui concerne la présence de B.
Discussion : Posé comme exigence, avec l'avertissement "facultatif". [Exigence 8.1.4]

A5. B informera A si il refuse la souscription de A.
Discussion : Posé comme exigence. [Exigence 5.1.5]

A6. Aucun tiers C ne peut forcer A à souscrire à la présence sans le consentement de A.
Discussion : Posé comme exigence. [Exigence 5.1.6]

A7. A peut annuler sa souscription à la présence de B à tout moment et pour n'importe quelle raison. Lorsque A le fait, elle ne va plus recevoir d'autres informations sur la présence de B.
Discussion : Cela se tient. Cependant, les mises en œuvre peuvent se trouver confrontées à des problèmes de fenêtre

temporelle lorsque A reçoit, après avoir envoyé sa demande d'annulation, une notification envoyée par B avant que celui-ci n'ait reçu la demande d'annulation. Donc, l'exigence devrait se concentrer sur le fait que B cesse d'envoyer les informations de présence, plutôt que sur le fait que A cesse de les recevoir. [Exigence 5.1.7]

A8. Aucun tiers C ne peut annuler la souscription de A à B.
Discussion : Tient comme exigence, bien que l'exception administrative s'applique . [Exigence 5.1.8]

A9. Il est notifié à A que sa souscription à B est annulée pour une raison quelconque.
Discussion : Bien que l'intention soit raisonnable, il y a un certain nombre de scénarios (par exemple, serveur surchargé, réseau obstrué, défaillance de serveur) où la livraison d'une notification à A de l'annulation est indésirable ou impossible. Donc, le service devrait tenter d'informer, mais cela n'est pas obligé. [Exigence 5.1.9]

Bob s'attend à ce que :

B1. B soit informé que A a souscrit aux informations de présence de B, pour autant que sa souscription n'est pas anonyme.
Discussion : Cette exigence tient. Cependant, B peut aussi choisir de déterminer la souscription de A après qu'elle soit effective. [Exigence 5.1.10]

B2. A soit identifiable et authentifié.
Discussion : Cela tient comme exigence. [Exigence 5.1.11]

B3. B puisse empêcher un usager particulier, D, de souscrire.
Discussion : Cela tient comme exigence. [Exigence 5.1.12]

B4. B puisse empêcher des usagers anonymes de souscrire.
Discussion : Cela tient comme exigence. [Exigence 5.1.13]

B5 Les informations de présence de B ne soient pas répétées par A à un tiers, E, qui n'y a pas souscrit.
Discussion : Ceci est pratiquement impossible à appliquer, de sorte que c'est omis de l'ensemble des exigences.

B6. B puisse refuser la souscription de A sans faire savoir à A qu'elle a été bloquée.
Discussion : Cette capacité de "blocage poli" tient essentiellement en acceptant qu'une souscription "refusée" ne devrait emporter aucune implication sur le service de ses notifications d'état. [Exigence 5.1.14]

B7. B puisse annuler à volonté la souscription de A.
Discussion : Tient comme exigence. [Exigence 5.1.15]

Charlie, l'administrateur de réseau de Bob s'attend à ce que :

C1. C sache qui a souscrit à B à tout moment.
Discussion : Les administrateurs devraient être capables de déterminer qui a souscrit, mais ils n'ont pas besoin d'être informés en continu de la liste des abonnés. Aussi, dans certains cas, les agents d'utilisateurs (par exemple, les mandataires) peuvent avoir souscrit au nom des utilisateurs, et dans ces cas, l'administrateur peut seulement déterminer l'identité de ces agents, et non celles de leurs utilisateurs. [Exigence 5.1.16]

C2. C puisse gérer tous les aspects des informations de présence de A.
Discussion : Cela tient comme exigence. [Exigence 5.1.17]

C3. C puisse contrôler qui a accès aux informations de présence de A et échanger des messages instantanés avec A.
Discussion : Cela tient en principe, mais C devrait être capable de renoncer à ces capacités si il le désire. [Exigence 5.1.18]

8.1.2 Publication

Bob, l'éditeur des informations d'état s'attend à ce que :

B1. Les informations sur B ne soient fournies à aucune entité sans le consentement et à l'insu de B.
Discussion : Ceci est presque impossible à réaliser et est donc omis des exigences.

8.1.3 Publication pour Notification

Lorsque des informations sont publiées pour notification, B s'attend à ce que :

B1. seule la personne A à qui la notification est envoyée puisse lire cette notification.
Discussion : Posé comme exigence. [Exigence 5.2.1]

B2. A reçoive fiablement toutes les notifications qui lui sont destinées.
Discussion : Cela tient, bien que "fiablement" soit un peu fort (par exemple, pannes du réseau, etc.). [Exigence 5.2.2]

B3. B puisse empêcher A de recevoir des notifications, même si A a normalement la permission de voir de telles notifications. Ceci est une variante du "blocage poli."
Discussion : Cela tient comme exigence. La notifications équivalente à la prochaine attente, B4 est aussi incorporée à cette exigence. [Exigence 5.2.3]

B4. B puisse fournir à deux parties intéressées A et E des informations d'état différentes au même moment. (B pourrait représenter différemment le même événement à deux personnes différentes.)
Discussion : Cela tient comme exigence ; elle a été incorporée dans l'exigence correspondante pour B3 ci-dessus.

B5. B s'attend à ce que C le malveillant ne puisse pas espionner les messages de notification sur B.
Discussion : Cela tient en principe, mais devrait être facultatif pour B. [Exigence 5.2.4]

8.1.4 Réception d'une Notification

Lorsque Alice reçoit une notification, le receveur, Alice, s'attend à ce que :

A1. les informations de notification soient précises et véritables.
Discussion : Cela tient en principe, bien qu'être "véritable" ne puisse être une exigence, et la vérification est facultative pour Alice. [Exigence 5.3.1]

A2. les informations sur les souscriptions restent privées ; les gens n'apprennent pas que la souscription de A aux informations de B existe en observant l'arrivée des notifications.
Discussion : Ceci est omis des exigences, car l'analyse de trafic, même de trafic chiffré, peut porter ces informations dans certaines situations.

A3. elle seule reçoive les notifications des choses auxquelles elle s'est abonnée.
Discussion : Tient comme exigence. [Exigence 5.3.2]

A4. les notifications viennent de l'envoyeur apparent, B.
Discussion : Tient en principe, bien que la vérification devrait être facultative pour A. [Exigence 5.3.3]

A5. A puisse dire la différence entre un message généré par l'utilisateur, et un message légitimement généré par l'agent au nom de l'utilisateur.
Discussion : Cela pourrait être assez difficile à mettre en application et pourrait indûment restreindre les scénarios d'utilisation ; c'est omis des exigences.

A6. les informations données par les agents au nom des utilisateurs puissent aussi être tenues pour véritables, complètes, et offertes à bon droit ; l'utilisateur ayant permis à l'agent de publier ces notifications.
Discussion : Ceci est difficile à mettre en application et est omis des exigences.

A7. A puisse prouver qu'une notification provenant de B a été livrée à temps et puisse prouver exactement combien de temps il a fallu pour la livraison du message.
Discussion : Ceci est difficile à mettre en application et est omis des exigences. Par exemple, une telle preuve pourrait impliquer un mécanisme de synchronisation mondial (car toutes les horloges système ont une incertitude associée) qui sort du domaine d'application du présent document.

A8. A puisse prouver que B était bien l'envoyeur d'un certain message.
Discussion : C'est une duplication de l'attente A4 ci-dessus et elle est reflétée dans l'exigence 5.3.3 correspondante.

8.2 Messages Instantanés

8.2.1 Messagerie Instantanée désignée

Lorsque l'usager Alice envoie un message instantané M à un autre usager Bob, Alice s'attend à :

A1. recevoir une notification de non livraison.
Discussion : Posé comme exigence. [Exigence 5.4.1]

Alice s'attend à ce que Bob :

B1. reçoive le message.
Discussion : C'est couvert par A1 et est reflété dans l'exigence 5.4.1 correspondante.

B2. reçoive le message rapidement.
Discussion : Posé comme exigence, bien que ce soit aussi couvert ailleurs (dans les exigences en dehors de la sécurité) de sorte que ceci est omis des exigences de sécurité.

B3. ne reçoive le message qu'une seule fois.
Discussion : Posé comme exigence. [Exigence 5.4.2]

B4. soit capable de vérifier qu'Alice a envoyé le message.
Discussion : Tient comme exigence. [Exigence 5.4.3]

B5. ne sache pas si il y a eu des copies conformes invisibles *(BCC)*.
Discussion : Émuler les conventions et protocoles sociaux de la messagerie électronique n'est pas une préoccupation centrale de cette initiative, et donc les références aux champs standard de la messagerie sont omises des exigences.

B6. soit capable de répondre au message.
Discussion : Tient en principe ; le receveur devrait être capable de répondre via un message instantané. [Exigence 5.4.4]

B7. sache si il était un receveur en copie cachée.
Discussion : Omis, comme noté ci-dessus.

B8. ne soit pas capable de déterminer d'informations sur A (comme sa localisation ou son adresse IP) sans la connaissance et le consentement de A.
Discussion : "des informations sur A" est trop général ; l'exigence devrait se concentrer sur l'adresse IP. De plus, "sans la connaissance et le consentement de A" peut être excessif. [Exigence 5.4.5]

Alice s'attend à ce qu'aucun autre usager Charlie ne soit capable de :

C1. voir le contenu de M.
Discussion : Tient en principe, bien que ceci ne devrait pas être obligatoire pour toutes les communications de messagerie instantanée. [Exigence 5.4.6]

C2. altérer M.
Discussion : Tient, avec le même avertissement que ci-dessus. [Exigence 5.4.7]

C3. sache que M a été envoyé.
Discussion : Il est impossible d'empêcher l'analyse de trafic, et ceci est donc omis des exigences.

Lorsque l'usager Bob reçoit un message instantané M d'un autre usager Alice, Alice s'attend à ce que Bob :

D1. soit capable de lire M.
Discussion : Posé comme exigence. [Exigence 5.4.8]

D2. soit capable de vérifier l'authenticité de M (aussi bien celle par rapport au temps qu'à l'identité de l'envoyeur).
Discussion : Comme noté précédemment, il n'est pas raisonnable d'exiger une vérification temporelle directe. Le protocole devrait, cependant, permettre de signer les messages en utilisant les normes de signature existantes. [Exigence 5.4.9]

D3. soit capable de vérifier l'intégrité de M.
Discussion : Tient comme exigence. [Exigence 5.4.10]

D4. soit capable d'empêcher A de lui envoyer d'autres messages.
Discussion : Posé comme exigence. [Exigence 5.4.11]

Bob s'attend à ce qu'Alice :

E1. avait l'intention d 'envoyer le message à Bob.

Discussion : Ceci est couvert par l'exigence 5.4.6 correspondante pour C1 ci-dessus.

E2. ait informé Bob de toutes les copies.
Discussion : Comme noté précédemment, les références aux copies sont omises des exigences.

8.2.2 Messagerie Instantanée anonyme

Discussion : La messagerie instantanée anonyme, comme dans "cacher l'identité de l'envoyeur", n'est pas réputée être une exigence centrale du protocole et les références y sont donc omises des exigences. Les mises en œuvre peuvent si elles le souhaitent fournir des facilités de messagerie anonyme, par des moyens qui doivent être cohérents avec les autres exigences.

Lorsque l'usager Alice envoie un message instantané anonyme à un autre usager, Bob, Alice s'attend à ce que Bob :
B1. reçoive le message ;
B2. reçoive rapidement le message ;
B3. reçoive le message une seule fois ;
AB4.1. ne puisse pas savoir qu'Alice l'a envoyé ;
AB4.2. sache que le message instantané est anonyme, et ne vient pas d'un usager spécifiquement désigné ;
AB4.3 puisse ne pas permettre les messages instantanés anonymes ;
B5. ne sache pas si il y a eu des copies conformes invisibles
B6. ne soit pas capable de répondre au message.

Alice s'attend à :
C1. recevoir une notification de non livraison.
AC2. recevoir une erreur si le message instantané a été refusé.

Bob s'attend à :
D1 être capable de lire M :
D2. être capable de vérifier l'authenticité de M (à la fois à l'égard de l'heure et de l'identité de l'envoyeur) ;
D3. être capable de vérifier l'intégrité de M ;
AD4. savoir si un IM a été envoyé en anonyme ;
AD5. être capable d'éliminer automatiquement la messagerie instantanée anonyme si il le désire ;
AD6. être capable de contrôler si une erreur est envoyée à Alice si M est éliminé.

8.2.3 Attentes de l'administrateur

Charlie, l'administrateur du réseau d'Alice s'attend à ce que :
C1. C soit capable d'envoyer des messages instantanés à A à tout moment ;
C2. A reçoive tout message qu'il envoie lorsque A est en ligne ;
C3. A ne soit pas capable de refuser la livraison d'un message instantané envoyé par C.

Discussion pour C1-C3 : On ne sait pas trop si cela a besoin d'un traitement spécial au niveau du protocole ; les administrateurs peuvent réaliser les objectifs ci-dessus par d'autres moyens. Par exemple, un administrateur peut envoyer un message à un utilisateur par les mécanismes normaux. Ces attentes ne figurent donc pas parmi les exigences.

Déclaration complète de droits de reproduction

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