Groupe de travail Réseau
Request for Comments : 5373
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

D. Willis, éditeur, Softarmor Systems
A. Allen, Research in Motion (RIM)

novembre 2008

Demande de modes de réponse pour le protocole d'initialisation de session (SIP)

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir 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 étend SIP avec deux champs d'en-tête et les étiquettes d'option associées qui peuvent être utilisés dans les demandes INVITE pour porter les préférences du demandeur sur le traitement de l'interface d'utilisateur relatives à la réponse à cette demande. Le premier en-tête, "Answer-Mode", exprime une préférence sur si l'interface d'utilisateur du nœud cible attend les entrées de l'utilisateur avant d'accepter la demande ou accepte plutôt la demande sans attendre l'entrée de l'utilisateur. Le second en-tête, "Priv-Answer-Mode", est similaire au premier, sauf qu'il demande un accès au niveau administratif et a par conséquent des exigences supplémentaires d'authentification et d'autorisation. Ces comportements concernent des applications comme celles de bouton poussoir et pour le diagnostic de retour en boucle. L'usage de chaque champ d'en-tête dans une réponse pour indiquer comment la demande a été traitée est aussi défini.

Table des matières

1. Fondements

Le modèle conventionnel pour l'établissement d'une session en utilisant le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261] implique 1) d'envoyer une demande de session (un INVITE) et de le notifier à l'utilisateur qui reçoit la demande, 2) l'acceptation de la demande et de la session par cet utilisateur, et 3) le renvoi d'une réponse (SIP 200 OK) au demandeur avant l'établissement de la session. Certains scénarios d'usage diffèrent de ce modèle, en particulier à l'égard de la phase de notification et d'acceptation. Bien qu'il ait toujours été possible au nœud qui reçoit la demande de sauter les phases de notification et d'acceptation, il n'y a pas de mécanisme standard pour que la partie qui envoie la demande indique spécifiquement le désir (ou l'exigence) de cette sorte de traitement. Le présent document définit un champ d'en-tête d'extension SIP qui peut être utilisé pour demander un traitement spécifique relatif à la phase de notification et d'acceptation.

Le premier scénario d'usage est l'exigence d'appels de diagnostic de bouclage. Dans cette sorte de scénario, un service d'essai envoie un INVITE à un nœud soumis à essai. Le nœud testé accepte et un dialogue est établi. Mais plutôt que d'établir un flux de supports bidirectionnel, le nœud testé met en boucle ou fait "écho" aux supports reçus du service d'essais vers le service d'essai. Le service d'essais peut alors analyser les caractéristiques de qualité et de délai des flux de supports. L'usage du protocole de description de session (SDP, *Session Description Protocol*) pour cette sorte de flux est décrit dans [LOOPBACK]. Dans cette sorte d'application, il pourrait n'être pas nécessaire que la personne qui utilise le nœud testé interagisse avec le nœud de quelque façon que ce soit pour que l'essai soit exécuté de façon satisfaisante. Dans certains cas, il pourrait être approprié d'alerter l'utilisateur de l'essai en cours, et dans d'autres cas cela ne le serait pas.

Le second scénario est celui des applications de bouton poussoir, qui ont été spécifiées par Open Mobile Alliance. Dans cette sorte d'environnement, SIP est utilisé pour établir un dialogue qui prend en charge la livraison asynchrone de flux de supports unidirectionnels, donnant une expérience d'utilisateur comme celle d'une radio traditionnelle bidirectionnelle. Il est de convention que les INVITE utilisés soient acceptés automatiquement par l'UA *(agent d'utilisateur)* appelé, et que le support soit couramment exécuté sur un haut-parleur. Le microphone de l'UA de l'appelé n'est pas engagé avant que l'utilisateur presse le bouton local "parler" pour répondre.

Un troisième scénario est celui du commutateur privé (PBX) participant. Les systèmes traditionnels de PBX professionnels incluent souvent une fonction d'intercommunication. Une utilisation normale de la fonction d'intercom est de permettre à un réceptionniste d'activer un haut parleur sur un téléphone de bureau afin d'annoncer un visiteur. Tous les appelants ne peuvent pas accéder au haut-parleur, seul le peut le réceptionniste ou l'opérateur, et on ne s'attend pas à ce que ces appelants veuillent toujours la fonction "intercom" – ils peuvent plutôt vouloir faire un appel ordinaire.

Il y a probablement beaucoup plus de cas d'utilisation pour les extensions définies dans cette spécification, mais ce document a été développé pour satisfaire spécifiquement les exigences de ces scénarios, ou d'autres avec des propriétés essentiellement similaires.

Ces sortes de mécanismes ne sont pas exigés pour fournir la fonction d'un "répondeur" ou "d'enregistreur de messagerie vocale". De tels appareils savent qu'on attend d'eux qu'ils répondent et n'exigent pas une extension à SIP pour prendre en charge ce comportement.

Beaucoup des discussions sur ce sujet dans les réunions du groupe de travail et sur la liste de diffusion ont porté sur la différence entre "mode réponse" et "mode d'alerte". Certains travaux préparatoires ne faisaient pas cette distinction. On donne les définitions suivantes :

- Le mode réponse inclut des comportements de l'UA SIP relatifs à l'acceptation ou au rejet d'une demande qui est contingente à l'interaction de l'UA et de l'utilisateur de cet UA après que l'UA a reçu la demande. On se soucie principalement de l'interaction avec l'utilisateur impliqué dans l'acceptation de la demande et qui initie une session active. Un exemple de cela pourrait être de presser le bouton "oui" d'un téléphone mobile.

- o le mode d'alerte inclut des comportements d'un UA SIP relatifs à l'information de l'utilisateur de l'UA qu'une demande d'initiation de session a été reçue. Un exemple de cela pourrait être d'activer la tonalité de sonnerie d'un téléphone mobile.

Le présent document traite seulement du "mode de réponse". Les questions relatives au "mode d'alerte" sortent de son domaine d'application.

Le présent document définit deux champs d'en-tête d'extension SIP : "Answer-Mode" *(mode Réponse)* et "Priv-Answer-Mode" *(mode de réponse privé)*. Ces deux extensions prennent les mêmes paramètres et opèrent de la même façon générale.

La distinction entre Answer-Mode et Priv-Answer-Mode se rapporte aussi au niveau d'autorisation exigé par le client d'agent d'utilisateur (UAC, *User Agent Client*) et qui est vérifié et régulé par le serveur d'agent d'utilisateur (UAS, *User Agent Server*). Les demandes sont généralement faites en utilisant le mode Réponse. Les demandes faites en utilisant le traitement Priv-Answer-Mode demandent un traitement "privilégié" de la part de l'UAS. Ce mécanisme est discuté plus en détails au paragraphe 4.1.

Le mode Priv-Answer n'est pas une assertion de privilège. C'est plutôt une demande de traitement privilégié. Ceci est similaire au modèle UNIX, où un utilisateur pourrait lancer une commande normale ou utiliser "sudo" pour demander un privilège administratif pour la commande. Inclure "Priv-" est équivalent à faire précéder une commande UNIX de "sudo". En d'autres termes, un tableau de politique séparé (comme "/etc/sudoers") est consulté pour déterminer si l'utilisateur peut recevoir le traitement demandé.

Cette distinction est discutée plus en détails au paragraphe 4.1.

1.1 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Syntaxe des champs d'en-tête et des étiquettes d'option

La syntaxe suivante utilise l'ABNF défini dans la [RFC5234]. De plus, il s'appuie sur la syntaxe pour SIP définie dans la [RFC3261]. La syntaxe des champs d'en-tête définis dans ce document est :

Answer-Mode = "Answer-Mode" HCOLON answer-mode-value *(SEMI answer-mode-param)

Priv-Answer-Mode = "Priv-Answer-Mode" HCOLON answer-mode-value *(SEMI answer-mode-param)

answer-mode-value = "Manual" / "Auto" / token

answer-mode-param= "require" / generic-param

L'étiquette d'option SIP qui indique la prise en charge de cette extension est "answermode".

Pour les mises en œuvre, les noms et valeurs de champ d'en-tête SIP sont toujours comparés de façon insensible à la casse. Les majuscules qui figurent ici sont seulement pour améliorer la lisibilité.

Cette syntaxe inclut des accroches d'extension ("token" pour les valeurs en mode réponse et "generic-param" pour les paramètres facultatifs) qui pourraient être définies à l'avenir. La présente spécification définit seulement le comportement pour les valeurs données explicitement ci-dessus. Afin d'assurer la rétro compatibilité, les mises en œuvre DOIVENT ignorer les valeurs inconnues.

3. Usage des champs d'en-tête Answer-Mode et Priv-Answer-Mode

Le présent document définit l'usage des champs d'en-tête Answer-Mode et Priv-Answer-Mode dans les demandes initiales (de formation du dialogue) SIP INVITE et dans les réponses 200 (OK) à ces demandes. Le présent document ne définit spécifiquement pas l'usage de toute autre sorte de demande ou réponse, incluant mais sans se limiter à ACK, CANCEL, ou tout usage de mi-dialogue.

Cette limitation découle de l'usage prévu de cette extension, qui est d'affecter la façon dont les utilisateurs interagissent avec les appareils de communication quand ils demandent de nouvelles sessions de communications et quand ils répondent à de telles demandes. Cette sorte d'interaction se produit seulement durant la formation d'un dialogue et son usage initial, et pas durant les opérations suivantes comme des re-INVITE. Cependant, les aspects de sécurité de l'initialisation de session doivent être appliqués aux changements de la description des supports introduite par les re-INVITES ou demandes similaires. Voir une discussion plus approfondie de cette question au paragraphe 7.1.

4. Usage des champs d'en-tête Answer-Mode et Priv-Answer-Mode dans les demandes

Le champ d'en-tête Answer-Mode ou Priv-Answer-Mode est utilisé par l'UAC dans une demande INVITE pour invoquer un traitement spécifique de la part de l'UAS répondant ; ce traitement se rapporte à la fonction de "réponse automatique" pour tout dialogue résultant de cette demande INVITE. Si aucun champ d'en-tête Answer-Mode ou Priv-Answer-Mode n'est inclus dans la demande, le comportement de réponse est à la discrétion de l'UAS, comme il le serait en l'absence de la présente spécification. Le traitement désiré est indiqué par la valeur du champ d'en-tête Answer-Mode ou Priv-Answer-Mode, comme suit :

Manuel : il est demandé à l'UAS de différer d'accepter la demande jusqu'à ce que l'utilisateur de l'UAS ait interagi avec l'interface d'utilisateur (UI) de l'UAS de façon à indiquer que l'utilisateur désire que l'UAS accepte la demande.

Auto : il est demandé à l'UAS d'accepter automatiquement la demande, sans attendre que l'utilisateur de l'UAS interagisse avec l'UI de l'UAS de façon à indiquer que l'utilisateur désire que l'UAS accepte la demande.

Chaque valeur du champ d'en-tête Answer-Mode ou Priv-Answer-Mode peut inclure un paramètre facultatif "require". Si il est présent, ce paramètre indique que l'UAC préférerait que l'UAS rejette la demande si l'UAS ne veut pas (peut-être à cause de sa politique) répondre dans le mode demandé, plutôt que de répondre dans un autre mode. Par exemple, ce paramètre pourrait être utilisé pour s'assurer qu'un appel d'essai de "rebouclage" ne perturbe pas un utilisateur qui a configuré son téléphone à répondre manuellement même si l'appelant demande une réponse automatique.

L'UAS est chargé de décider comment honorer cette préférence. En général, l'UAS prend une décision d'autorisation sur la base de l'identité authentifiée présentée dans la demande en utilisant des mécanismes d'authentification comme l'authentification par résumé SIP [RFC3261], le mécanisme d'identité SIP [RFC4474], ou (dans les réseaux restreints pour lesquels il convient) le mécanisme SIP pour l'identité affirmée au sein de réseaux de confiance [RFC3325]. Quand il prend une décision d'autorisation, l'UAS devrait aussi utiliser les informations d'autorisation ou de politique disponibles. Ces prises de décision DOIVENT considérer le modèle de risque de la session correspondant à la demande, et l'UAS NE DOIT PAS répondre sans apport de l'utilisateur dans les cas où la confidentialité ou la sécurité de l'utilisateur pourrait en être compromise. Cette détermination est l'affaire du système ou de la conception de l'application, et ne peut en général pas être traitée en ayant un ensemble de fonctions dont l'activation ou la désactivation est configurable. Une discussion spécifique des sessions de support et de la politique appropriée est présentée à la Section 7.

4.1 Différence entre mode Réponse et mode Priv-Answer

Les fonctions des champs d'en-tête Answer-Mode et Priv-Answer-Mode sont similaires ; elle demandent toutes deux que l'UAS traite la demande comme spécifié par la valeur du champ d'en-tête (automatique ou manuel). La différence est dans la façon dont la demande interagit avec la politique de l'UAS. Un UAS typique va avoir des politiques différentes pour traiter chaque champ d'en-tête. Par exemple, en supposant que l'utilisateur d'un UAS a placé cet UAS en "mode réunion", indiquant qu'il est engagé dans une activité importante et ne souhaite pas être interrompu. L'UAS pourrait interdire la réponse automatique pour les demandes en Answer-Mode quand il est en "mode réunion". Cependant, cet UAS pourrait permettre la réponse automatique pour les demandes faites avec le mode Priv-Answer. Il va probablement y avoir des différences dans la politique d'autorisation. Par exemple, un UAS pourrait être configuré de telle façon que les appelants sur la liste "amis" soit admis à faire des demandes en utilisant le mode Réponse mais pas le mode Priv-Answer. Ce même UAS pourrait être configuré à seulement permettre aux appelants sur la liste "administrateurs" d'utiliser le mode Priv-

Answer. Ceci est différent de toujours fonder le comportement sur l'identité de l'appelant. Par exemple, supposons que l'appelant "Bob" soit sur les deux listes "amis" et "administrateurs". Si Bob veut que sa demande soit traitée en accord avec la politique normale, il utilise le mode Réponse. Si Bob veut que sa demande soit traitée selon la politique plus restrictive "privilégiée", il utilise le mode Priv-Answer.

Un UAS DEVRAIT appliquer une politique plus stricte d'autorisation à une demande avec le mode Priv-Answer qu'il ne le fera avec des demandes en mode Réponse. La politique par défaut DEVRAIT être de refuser les demandes contenant des champs d'en-tête Priv-Answer-Mode sauf si le demandeur est authentifié et spécifiquement autorisé à faire des demandes en mode Priv-Answer. Manquer à appliquer une telle politique laisse l'utilisateur potentiellement vulnérable aux abus, comme discuté à la Section 7.

Le cas d'utilisation envisagé pour le mode Priv-Answer se rapporte au traitement de demandes urgentes d'appelants autorisés. Par exemple, supposons que Larry soit un conducteur de limousine travaillant avec un répartiteur de flotte. Larry aime fournir un environnement tranquille pour sa voiture, de sorte que son communicateur est configuré pour un mode de réponse manuel pour tous les appels non privilégiés, incluant des appels de bouton poussoir (mode de réponse : automatique). Chaque fois qu'il a un appel, le communicateur de Larry carillonne doucement pour l'alerter de l'appel. Si les circonstances le permettent, Larry presse le bouton du communicateur pour accepter l'appel, le communicateur envoie une réponse 200 (OK) et le bouton d'appel de l'appelant est activé par le haut parleur du communicateur. Ce traitement est fourni aux demandes entrantes qui ont le champ d'en-tête Answer-Mode de valeurs "Manuel" ou "Automatique" (ou pas de champ d'en-tête mode Réponse du tout) quel que soit l'appelant.

L'opérateur de répartition de flotte de Larry est familiarisé avec cette politique, et a besoin d'informer Larry d'une affaire critique. L'opérateur de répartiteur essaye plusieurs fois le bouton poussoir pour appeler Larry (incluant le mode réponse : Auto dans les demandes) mais les appels ne sont pas acceptés parce que Larry s'est endormi, et donc il ne presse pas le bouton de son communicateur pour accepter l'appel.

L'opérateur presse alors son bouton "urgent" et rappelle encore Larry. Cette fois, la demande INVITE porte un champ d'en-tête "Priv-Answer-Mode: Auto". Le communicateur de Larry vérifie l'identité de l'appelant (en utilisant une assertion d'identité SIP ou un mécanisme de fonction équivalente) et confronte l'identité de l'opérateur à la liste des utilisateurs admis au mode Priv-Answer. Comme l'opérateur est sur la liste, le communicateur retourne immédiatement une réponse 200 (OK) acceptant l'appel. L'opérateur parle, et la salve de parole résultante est exécutée sur le haut parleur du communicateur de Larry, ce qui le réveille.

L'effet de demander le mode Priv-Answer est différent de celui de simplement accorder un privilège supérieur à une demande en mode Réponse fondé sur l'identité du demandeur et du niveau d'autorisation correspondant. Cette distinction est ce qui permet à l'opérateur de flotte de faire des demandes polies (mode Réponse : Auto) à Larry dans des conditions normales, et de recevoir un traitement différent (Priv-Answer-Mode : Auto) pour une demande d'urgence supérieure.

En fonctionnement normal, seulement un des modes Réponse ou Priv-Answer serait utilisé dans une demande INVITE. Si les deux sont présents, l'UAS va d'abord vérifier l'autorisation du demandeur pour le mode Priv-Answer et, si il est autorisé, traiter la demande comme si seulement le mode Priv-Answer avait été inclus. Si le demandeur n'est pas autorisé pour le mode Priv-Answer, alors l'UAS va traiter la demande comme si seulement le mode Réponse était inclus.

4.2 Modificateur "require"

Les deux modes Réponse et Priv-Answer permettent un modificateur "require" (exemple : "Priv-Answer-Mode: Auto;require"). Ce modificateur n'influence pas la politique de l'UAS pour choisir si il répond manuellement ou automatiquement. L'UAS décide si il répond ou non automatiquement sur la base d'autres aspects de la demande. Le modificateur "require" est seulement évalué après que l'UAS a choisi un mode de réponse. Si la politique de l'UAS a résulté en un mode de réponse qui est différent de celui spécifié dans la demande, la présence du modificateur "require" demande à l'UAS de rejeter l'appel. Dans l'exemple donné, il est demandé à l'UAS de répondre automatiquement si l'appelant est autorisé à une réponse automatique dans la politique "privilégié", et de rejeter l'appel (plutôt que de répondre manuellement) si l'appelant n'est pas autorisé pour ce mode. Ceci est discuté plus en détails au paragraphe 4.5.

4.3 Procédures au client d'agent d'utilisateur

4.3.1 Toutes les demandes

Un UA qui prend en charge les champs d'en-tête Answer-Mode et Priv-Answer-Mode DEVRAIT indiquer son soutien en

incluant une étiquette d'option de "answermode" dans le champ d'en-tête Supported de toutes les demandes qu'il envoie.

4.3.2 Transactions REGISTER

Pour indiquer qu'il prend en charge la caractéristique de négociation du mode Réponse, un UA PEUT inclure un paramètre extensions avec une valeur qui inclut "answermode". Exemple :

;extensions="answermode,100rel,gruu"

dans le champ d'en-tête Contact de ses demandes REGISTER. Cet usage des étiquettes de caractéristiques est décrit dans la [RFC3840].

Si un UA dépend de la prise en charge des capacités d'appelant chez le registraire, il PEUT inclure un champ d'en-tête Require avec la valeur de "pref" dans sa demande REGISTER. Cela va causer le rejet par le registraire de la demande si le registraire ne prend pas en charge les capacités de l'appelé et les préférences de l'appelant. Exemple :

Require: pref

4.3.3 Transactions INVITE

Un UAC qui prend en charge la présente spécification PEUT inclure un champ d'en-tête Answer-Mode ou Priv-Answer-Mode dans un INVITE lorsque il souhaite influencer le mode de réponse de l'UAS qui répond.

Note : Ceci n'a un sens que dans les demandes INVITE initiales ou de formation de dialogue. Les champs d'en-tête Answer-Mode et Priv-Answer-Mode qui apparaissent dans d'autres demandes sont ignorés. En général, si la demande ne résulterait normalement pas en une notification à l'utilisateur et à l'acceptation par cet utilisateur (par exemple, "ringing" et "answering") ces extensions ne sont alors pas applicables.

Pour demander que l'UAS réponde seulement après avoir interagi avec son utilisateur et avoir reçu une instruction affirmative de cet utilisateur, l'UAC inclut un champ d'en-tête Answer-Mode ou Priv-Answer-Mode d'une valeur de "Manual". Exemple :

Answer-Mode: Manual

Pour demander que l'UAS réponde manuellement, et demander qu'il rejette la demande INVITE si il est incapable ou ne veut pas répondre manuellement, l'UAC inclut un champ d'en-tête Answer-Mode ou Priv-Answer-Mode de valeur "Manual" et un paramètre "require". Exemple :

Answer-Mode: Manual;require

Pour demander que l'UAS réponde automatiquement sans attendre une entrée de l'utilisateur, l'UAC inclut un champ d'en-tête Answer-Mode ou Priv-Answer-Mode de valeur "Auto". Exemple :

Answer-Mode: Auto

Pour demander que l'UAS réponde automatiquement, et demander qu'il rejette la demande INVITE si il est incapable ou ne veut pas répondre automatiquement, l'UAC inclut un champ d'en-tête Answer-Mode ou Priv-Answer-Mode de valeur "Auto" et un paramètre "require". Exemple :

Answer-Mode: Auto;require

Pour exiger que l'UAS prenne en charge cette extension ou rejette la demande, l'UAC inclut un champ d'en-tête Require avec la valeur de "answermode". Cela ne force pas réellement l'UAS à répondre automatiquement, cela exige juste que l'UAS comprenne cette extension ou rejette la demande. On n'a pas de technique de négociation SIP pour forcer un comportement spécifique. Le comportement désiré est plutôt indiqué dans l'extension SIP elle-même. Exemple :

Require: answermode

Pour demander que les mandataires de reciblage sur le chemin choisissent de préférence les cibles qui ont indiqué la prise

en charge de cette extension dans leur enregistrement, un UAC inclut un champ d'en-tête Accept-Contact avec un paramètre d'extensions de valeur "answermode". Cet usage de Accept-Contact est décrit dans la [RFC3841]. Cela va normalement être utilisé en conjonction avec le champ d'en-tête "Require: answermode" comme décrit ci-dessus. Exemple :

Require: answermode Accept-Contact: *;extensions="answermode";methods="INVITE"

Pour demander que les mandataires de reciblage sur le chemin ne choisissent pas les cibles qui ont indiqué la non prise en charge de cette extension dans leur enregistrement, un UAC inclut un champ d'en-tête Accept-Contact avec un paramètre d'extensions de valeur "answermode" et un champ d'option de "require". Cet usage de Accept-Contact est décrit dans la [RFC3841]. Cela va normalement être utilisé en conjonction avec le champ d'en-tête "Require: answermode" comme décrit ci-dessus. Exemple :

Require: answermode Accept-Contact: *;extensions="answermode"; methods="INVITE";require

Pour demander que les mandataires de reciblage sur le chemin choisissent exclusivement les cibles qui ont indiqué la prise en charge de cette extension dans leur enregistrement, un UAC inclut un paramètre d'extensions de champ d'en-tête Accept-Contact d'une valeur de "answermode" et les options "require" et "explicit". Cet usage de Accept-Contact est décrit dans la [RFC3841]. Cela va normalement être utilisé en conjonction avec le champ d'en-tête "Require: answermode" comme décrit ci-dessus. Exemple :

Require: answermode Accept-Contact: *;extensions="answermode"; methods="INVITE";require;explicit

4.4 Procédures des mandataires intermédiaires

4.4.1 Comportement général du mandataire

La procédure générale pour tous les mandataires intermédiaires, y compris le ou les mandataires qui desservent l'UAC et le ou les mandataires qui desservent l'UAS, est d'ignorer le champ d'en-tête Answer-Mode. Cependant, les mandataires desservants (mandataires responsables de la résolution d'une adresse d'enregistrement (AOR) dans un contact enregistré) PEUVENT exercer un contrôle sur le mode de réponse demandé, soit en insérant ou supprimant un champ d'en-tête Answer-Mode ou Priv-Answer-Mode, soit en altérant la valeur d'un champ d'en-tête existant, en accord avec la politique locale. Il pourrait en résulter un comportement différent de l'attente de l'utilisateur (comme d'avoir un appel qui était destiné à être un rebouclage de diagnostic auquel répond une personne) et par conséquent les mandataires NE DOIVENT PAS insérer, supprimer, ou altérer les champs d'en-tête Answer-Mode ou Priv-Answer-Mode sauf autorisation explicite de le faire par un accord externe de l'opérateur du mandataire et de l'utilisateur de l'UA que le mandataire dessert. Ces mandataires desservants PEUVENT aussi rejeter une demande selon la politique locale et, si ils le font, ils DEVRAIENT utiliser les codes de rejet spécifiés ci-dessous pour l'UAS.

4.4.2 Problèmes du répondeur automatique et du fourchement

Un des problèmes bien connus du fourchement est celui de l'acceptation multiple. Si une demande INVITE est fourchée sur plusieurs UAS et si plus d'un répond avec un 200 (OK) l'approche conventionnelle est de continuer le dialogue avec le premier qui répond et de supprimer le dialogue (avec des demandes BYE) avec tous les autres répondants.

Bien que ce problème existe sans la capacité de négociation d'auto-réponse, il apparaît que l'adoption large d'UA qui engagent un comportement d'auto-réponse va exacerber le problème de la multi acceptation. Par conséquent, les concepteurs de systèmes doivent prendre en compte cet aspect. En général, l'auto-réponse n'est PAS RECOMMANDÉE dans les environnements qui incluent du fourchement en parallèle.

Comme solution de remplacement, il pourrait être raisonnable d'utiliser une variante de la réponse manuelle combinée avec l'absence d'alerte et un support précoce. Dans cette approche, le message initial ou la salve de parole est transmis comme support précoce à tous les receveurs, où il est affiché ou exécuté. Toute expression de réponse (pousser la clé d'émission et parler) de la part de l'utilisateur d'un UAS à la suite de cela servirait "d'acceptation", résultant en une réponse 200 (OK) transmise par leur UAS. Par conséquent, le conflit d'acceptation va être limité au sous ensemble des UA répondant réellement sous le contrôle de l'utilisateur, plutôt que tout l'ensemble des UA auxquels la demande a fourché.

Une autre solution de remplacement serait d'utiliser la conférence dynamique au lieu du fourchement. Dans cette approche, au lieu de fourcher la demande, une conférence serait initiée et tous les UA enregistrés seraient invités à cette conférence. Le mixeur attaché à la conférence régulerait alors les flux de trafic de façon appropriée.

4.5 Procédures des serveurs d'agent d'utilisateur

4.5.1 Transactions INVITE

Pour une demande qui a une valeur de Answer-Mode de "Manual" et n'a pas de paramètre Answer-Mode de "require", l'UAS DEVRAIT différer d'accepter la demande jusqu'à ce que l'utilisateur de l'UAS ait confirmé sa volonté d'accepter la demande. Ce comportement PEUT être altéré comme nécessaire pour les UAS non participants ou d'autres caractéristiques ou politiques locales. Par exemple, un auto-participant ou un système de passerelle de réseau téléphonique public commuté (RTPC) qui répond toujours automatiquement va répondre , en dépit de la présence de la valeur de champ d'en-tête mode Réponse "Manual".

Pour une demande qui a une valeur de mode Réponse de "Manual" et un paramètre Answer-Mode de "require", l'UAS DOIT différer d'accepter la demande jusqu'à ce que l'utilisateur de l'UAS ait confirmé sa volonté d'accepter la demande. si l'UAS n'est pas capable de répondre à la demande dans ce mode "Manual" ou ne veut pas le faire, il DOIT rejeter la demande, DEVRAIT le faire avec une réponse "403 (Interdit)", et PEUT inclure une raison de "Réponse manuelle interdite".

Pour une demande qui a une valeur de Answer-Mode de "Auto", l'UAS DEVRAIT, si l'appelant est authentifié et autorisé pour la réponse automatique, accepter la demande sans autre entrée de l'utilisateur. L'UAS PEUT, en accord avec la politique locale ou les préférences de l'utilisateur, traiter cette demande comme il le ferait d'une demande ayant un mode Réponse de valeur "Manual" ou n'ayant pas de champ d'en-tête. Si l'appelant n'est pas authentifié et autorisé pour la réponse automatique, l'UAS PEUT traiter la demande comme pour "manual", ou rejeter la demande. Si l'UAS rejette la demande, il DEVRAIT le faire avec une réponse "403 (Interdit)", et PEUT inclure une raison de "Réponse automatique interdite". Il peut y avoir une interaction avec le paragraphe 23.2 de la [RFC3261], qui dans certains cas exige que l'utilisateur valide les certificats utilisés pour S/MIME. Comme cela fait peser la même charge d'interruption sur l'utilisateur que la réponse manuelle à la demande, un UAS qui rencontre cette exigence pour la validation par l'utilisateur d'une demande qui exige une réponse automatique DEVRAIT rejeter la demande avec une réponse "403 (Interdit)" et PEUT inclure une raison de "La validation de certificat exige une entrée de l'utilisateur non compatible avec une réponse automatique".

Pour une demande qui a une valeur de Answer-Mode de "Auto" et un paramètre Answer-Mode de "require", l'UAS DEVRAIT, si l'appelant est authentifié et autorisé pour la réponse automatique, accepter la demande. L'UAS NE DOIT PAS permettre la réponse "manual" à cette demande, mais PEUT la rejeter. Si, pour une raison quelconque, l'UAS choisit de ne pas accepter automatiquement la demande, il DOIT rejeter la demande, DEVRAIT le faire avec une réponse "403 (Interdit)", et PEUT inclure une raison de "Réponse automatique interdite".

Un comportement similaire s'applique pour le mode Priv-Answer, sauf que la politique pour l'autorisation peut être différente (et généralement plus stricte).

5. Usage des champs d'en-tête Answer-Mode et Priv-Answer-Mode dans les réponses

Le champ d'en-tête Answer-Mode ou Priv-Answer-Mode peut être inséré par un UAS dans une réponse afin d'indiquer comment il a traité la demande associée à l'égard de la fonction de réponse automatique. L'UAC peut utiliser cette information pour informer l'utilisateur ou autrement adapter le comportement de l'interface d'utilisateur. Le traitement est indiqué par la valeur du champ d'en-tête, comme suit :

Manuel : l'UAS a répondu après que l'utilisateur de l'UAS a interagit avec l'interface d'utilisateur (UI) de l'UAS de façon à indiquer que l'utilisateur désire que l'UAS accepte la demande.

Auto : l'UAS a répondu automatiquement, sans attendre que l'utilisateur de l'UAS interagisse avec l'UI de l'UAS de façon à indiquer que l'utilisateur désire que l'UAS accepte la demande.

Les champs d'en-tête Answer-Mode et Priv-Answer-Mode, quand ils sont utilisés dans les réponses, ne sont valides que dans une réponse 200 (OK) à une demande INVITE.

5.1 Procédures à l'UAS

Un UAS qui prend en charge la présente spécification insère un champ d'en-tête Answer-Mode ou Priv-Answer-Mode dans la réponse 200 (OK) à une demande INVITE quand il souhaite informer l'UAC de si la demande a reçu une réponse manuelle ou automatique. Il est raisonnable pour un UAS de supposer que si l'UAC a inclus un champ d'en-tête Answer-Mode dans la demande, il voudrait probablement voir un champ d'en-tête Answer-Mode dans la réponse. Toutes les raisons d'inclure ou non ce champ d'en-tête dans une réponse sortent du domaine d'application de cette spécification, et sont en relation avec les problèmes de confidentialité de l'utilisateur de l'UAS. Par exemple, informer l'appelant qu'un appel a reçu une réponse manuelle peut révéler la présence d'un "humain réel" à l'UAS qui répond. Bien qu'en général, la conversation qui s'ensuit révèle aussi cette même information, il peut y avoir des cas où cette information pourrait devoir être protégée. Par conséquent, les UAS qui prennent en charge la présente spécification DEVRAIENT inclure les mécanismes de politique configurables de façon appropriée pour faire cette détermination, et la configuration par défaut DEVRAIT être d'exclure ce champ d'en-tête des réponses.

5.2 Procédures à l'UAC

Un UAC PEUT utiliser la valeur du champ d'en-tête Answer-Mode ou Priv-Answer-Mode, si il est présent, pour adapter l'interface d'utilisateur et/ou informer l'utilisateur sur le traitement de la demande. Par exemple, l'utilisateur d'un système à bouton poussoir pourrait parler différemment si il sait que l'appelé a répondu "en personne" plutôt que d'avoir l'appel qui débouche sur un téléphone sans personne au bout.

6. Exemples d'utilisation

Les exemples suivants montrent Bob enregistrant un contact qui prend en charge la négociation du mode Réponse. Alice appelle alors Bob avec une demande INVITE, demandant une réponse automatique et demandant explicitement que la demande ne soit pas acheminée aux contacts qui n'ont pas indiqué la prise en charge de cette extension. De plus, Alice exige que la demande soit rejetée si l'UA de Bob ne prend pas en charge la négociation du mode Réponse. Bob réplique avec une réponse 200 (OK) indiquant que l'appel a eu une réponse automatique.

Le champ d'en-tête Content-Length montré dans les exemples contient un bouche-trou "..." à la place d'un Content-Length valide. De plus, les corps SDP qui seraient attendus dans les demandes INVITE et les réponse 200 (OK) ne sont pas montrées.

6.1 Demande REGISTER

Dans l'exemple suivant, l'UA de Bob s'enregistre et indique qu'il prend en charge l'extension "answermode".

```
REGISTER sip:exemple.com SIP/2.0
From: Bob<sip:bob@exemple.com>
To: Bob <sip:bob@exemple.com>
CallID: hh89as0d-asd88jkk@cell-phone.exemple.com
CSeq: 1 REGISTER
Contact: sip:cell-phone.exemple.com;
  ;audio
  ;+sip.extensions="answermode"
  ;methods="INVITE,BYE,OPTIONS,CANCEL,ACK"
  ;schemes="sip"
```

6.2 Demande INVITE

Dans cet exemple, Alice appelle Bob et demande à l'UA de Bob de répondre automatiquement. Cependant, Alice veut que Bob réponde manuellement si la politique de Bob est de préférer la réponse manuelle, de sorte que Alice n'inclut pas de modificateur ";require" sur le "Answer-Mode: Auto".

```
INVITE sip:bob@exemple.com SIP/2.0
Via: SIP/2.0/TCP client-alice.exemple.com:5060; branch=z9hG4bK74b43
Max-Forwards: 70
From: Alice <sip:alice@atlanta.exemple.com>;tag=9fxced76sl
```

To: Bob <sip:bob@exemple.com>
Call-ID:3848276298220188511@client-alice.exemple.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.exemple.com;transport=tcp>
Require: answermode
Accept-contact:*;require;explicit;extensions="answermode"
Answer-Mode: Auto
Content-Type: application/sdp
Content-Length: ...

6.3 Réponse 200 (OK)

Ici, Bob a accepté l'appel et son UA a répondu automatiquement, ce qu'il indique dans la réponse 200 (OK).

SIP/2.0 200 OK
Via: SIP/2.0/TCP client-alice.exemple.com:5060; branch=z9hG4bK74b43
From: Alice <sip:alice@exemple.com>;tag=9fxced76sl
To: Bob <sip:bob@exemple.com>;tag=8321234356
Call-ID: 3848276298220188511@client-alice.exemple.com
CSeq: 1 INVITE
Contact: <sip:bob@client.biloxi.exemple.com;transport=tcp>
Answer-Mode: Auto
Content-Type: application/sdp
Content-Length: ...

7. Considérations sur la sécurité

La présente spécification ajoute la capacité pour un UAC de demander un comportement d'interface d'utilisateur potentiellement risqué à l'égard de l'acceptation d'une demande INVITE par l'UAS qui reçoit la demande. Spécifiquement, l'UAC peut demander que l'UAS accepte la demande sans entrée à l'UAS par l'utilisateur de l'UAS (Answer-Mode: Auto).

Il y a ici plusieurs attaques possibles – la plus évidente étant la capacité de mettre un téléphone en écoute à distance sans que l'utilisateur le sache. Des attaques potentielles supplémentaires incluent la fraude d'inversion de charges, de communications de bouton poussoir non sollicitées (pourriels sur bouton poussoir (SPTT, *spam over push-to-talk*)), exécution de bruits odieux (l'attaque du "coussin péteur"), le déni de service de batterie à plat, le déni de service de "occupé forcé", d'augmentation de la facture de transport de données de la victime, et l'hameçonnage via l'insertion de session (où une session en cours est remplacée par une autre sans que la victime le sache).

Comme les mises en œuvre de SIP n'utilisent généralement pas la protection de message de bout en bout, la présente spécification dépend complètement de la sécurité transitive à travers les mandataires SIP. Tout mandataire qui se comporte mal peut insérer, supprimer, et/ou altérer le contenu des champs d'en-tête Answer-Mode et Priv-Answer-Mode, et en général peut le faire sans être remarqué par l'UAC ou l'UAS. Par conséquent, il est critique que tout mandataire sur le chemin soit non seulement de confiance mais aussi digne de cette onfiance. Bien que les mandataires n'insèrent, suppriment ou altèrent généralement pas intentionnellement de champs d'en-tête Answer-Mode et Priv-Answer-Mode, la présente spécification note un cas d'utilisation de manipulation par des mandataires agissant au nom de l'utilisateur d'un UAC ou UAS qui a une prise en charge limitée de l'authentification ou de l'application de politique nécessaires pour exercer en toute sécurité ces extensions. Les mandataires qui effectuent une telle manipulation d'extension sensible DOIVENT donc fournir une application complète de la politique, conformément à la politique minimale discutée au paragraphe 7.4.

Le corpus existant des travaux sur SIP donne de fortes capacités d'authentification des demandes, de prévention des attaques par interposition, de protection de la confidentialité et de l'intégrité des flux de supports, et ainsi de suite (bien que, comme noté ci-dessus, ces capacités s'appuient généralement sur une confiance transitive entre les mandataires). Les comportements ajoutés par les extensions de ce document soulèvent des possibilités supplémentaires d'attaques contre les flux de supports qui ne sont pas complètement traités par les travaux existants sur SIP, et donc exigent d'être analysés par ce document.

Les attaques sur les supports peuvent être en gros catégorisées comme :

Insertion : des supports sont insérés dans l'UA de la victime et exécutés sans le consentement de l'utilisateur de l'UA.

Interception : la facilité d'acquisition de supports de l'UA victime (comme un microphone ou une caméra) est activée, produisant un flux de supports, sans le consentement de l'utilisateur de l'UA.

7.1 La sensibilité à l'attaque dépend des caractéristiques du support

Le danger d'abus varie largement selon les caractéristiques des support de la session établie. Comme la gamme d'expression des sessions de supports qui peut être établie par SIP est illimitée, on peut trouver plus efficace de modéliser les catégories de modalités de supports plutôt que de décrire explicitement chaque scénario possible. L'analyse de la sécurité peut alors être appliquée par modalité.

Les modalités de support intéressantes paraissent être :

Insertion de supports unidirectionnels générés par l'UAC (entrants) : des flux de supports sensibles provenant de l'UAC et sont rendus par l'UAS, perturbant l'utilisateur de l'UAS ou interrompant les fonctions de l'UAS. On appelle cela l'attaque du "coussin péteur" à cause de son utilisation dans la réplique du coussin qui fait des bruits incongrus. Le danger de cette attaque est assez littéralement amplifié par un haut parleur rattaché à l'UAS victime. Le support qui a une implication secondaire minimale (comme d'envoyer un coup dans un jeu d'échecs à un ordinateur qui ne fait pas fonctionner de jeu d'échec) est relatif, mais de moindre signification Cette sorte d'attaque peut aussi avoir d'autres conséquences, comme de décharger la batterie de la victime ou d'augmenter les charges de transport de données à payer par la victime.

Interception de supports unidirectionnels générés par l'UAC (sortants) : des flux de supports sensibles provenant de l'UAS et sont rendus pat l'UAC, violant la confidentialité de l'utilisateur de l'UAS. On se réfère à cela sous le nom d'attaque de la "punaise dans le téléphone" parce que cela va apparaître comme la principale motivation de l'attaque.

Insertion ou interception de support bidirectionnel : le support bidirectionnel est le cas courant où SIP est utilisé dans un scénario de voix sur IP ou "d'appel téléphonique traditionnel". Une fois qu'un flux de supports est établi, les deux côtés envoient et reçoivent des supports sans autre engagement. Les informations de supports sont présumées sensibles -- c'est-à-dire, si elles sont interceptées cela cause des dommages à la vie privée de la victime, et si elles sont insérées, cela perturbe ou interfère avec le receveur. Les attaques de cette sorte pourraient produire des scénarios de "coussin péteur" ou de "punaise dans le téléphone", potentiellement simultanément.

Il semble raisonnable de considérer l'attaque de "punaise dans le téléphone" comme étant d'une classe différente (potentiellement beaucoup plus sévère) que celle du "coussin péteur". Cette distinction suggère que la politique de sécurité pourrait être établie d'une façon différente et probablement moins restrictive pour les flux de supports entrants que pour les flux de supports sortants. L'ensemble d'appelants de qui un utilisateur va vouloir accepter automatiquement des supports entrants est raisonnablement beaucoup plus large que l'ensemble d'appelants auxquels un utilisateur va vouloir accorder automatiquement l'accès aux supports sortants, bien que ceci puisse n'être pas vrai dans tous les environnements, en particulier ceux où la réception de supports non voulus a des conséquences financières non désirées.

Par exemple, supposons qu'un UA soit conçu de telle façon qu'il puisse être utilisé pour recevoir des appels de bouton poussoir à un haut-parleur, et qu'il puisse être utilisé comme un "surveillant de bébé" (il a un microphone ouvert et écoule les sons audio reçus à celui qui écoute). La politique pour activer le haut parleur à bouton poussoir va probablement devoir être raisonnablement large (peut-être "tous les amis de l'utilisateur"). Cependant, la politique pour le surveillant de bébé doit être très serrée (peut-être "seulement la maman du bébé") ou même complètement fermée. La politique minimale définie au paragraphe 7.4 interdit explicitement la fonction de "surveillant de bébé".

7.2 La conception de l'application affecte l'opportunité d'attaque

Dans les cas d'utilisation les plus courants, les aspects de sécurité sont un peu atténués par les aspects de conception de l'application. Par exemple, dans la téléphonie traditionnelle, l'appelé est alerté par la demande (le téléphone sonne) aucune session de support n'est établie sans l'acceptation de l'appelé (qui décroche le téléphone) et le chemin des supports est très couramment livré à un seul combiné d'utilisateur. Par conséquent, cette application (bien que bidirectionnelle) est relativement sûre contre les attaques d'insertion et d'interception de supports de la sorte qui est activée par les extensions de ce document. L'utilisation d'appareils de réponse automatique sans politique (comme les répondeurs) et d'amplification

(appareils de microphone et de visualisation d'appel) affaiblit cette défense.

Dans les applications de bouton poussoir, le support peut être envoyé de l'UAC à l'UAS sans connaissance de l'utilisateur , mais aucun support n'est envoyé de l'UAS appelé sans entrée de l'utilisateur (la "poussée" du "bouton poussoir"). Par conséquent, il n'y a pas d'opportunité d'attaque de "punaise dans le téléphone". De plus, l'examen par l'UAC qui élimine les identités d'UAC qui ne sont pas sur une sorte de "liste blanche" (souvent, une liste des amis) réduit la menace d'attaques de "coussin péteur" (sauf de la part des amis, bien sûr).

Des approches similaires s'appliquent à la plupart des applications. L'insertion peut être contrôlée (mais pas éliminée) en combinant les mécanismes d'identité avec une simple politique d'autorisation, et l'interception peut être effectivement éliminée en combinant de forts mécanismes d'identité avec une politique d'autorisation agressive et/ou une interaction de l'utilisateur.

7.3 Application de l'analyse

Les extensions décrites dans ce document donnent des mécanismes par lesquels un UAC peut demander qu'un UAS ne déploie pas deux des cinq mécanismes défensifs mentionnés ci-dessous – l'alerte de l'utilisateur et l'acceptation de l'utilisateur. Afin que cela ne produise pas un risque exagéré d'attaque d'insertion ou un risque accru d'attaque d'interception, on est donc forcé de s'appuyer sur les mécanismes défensifs restants. Le présent document définit un seuil minimum pour une sécurité satisfaisante. Des politiques certainement plus restrictives pourraient raisonnablement être utilisées, mais toute politique moins restrictive que l'approche décrite ci-dessous va très probablement résulter en problèmes de sécurité significatifs.

De la discussion précédente des risques, attaques, et vulnérabilités, on peut déduire cinq mécanismes défensifs disponibles au niveau application :

1. Identité – savoir de qui vient la demande.

2. Alerte – faire que l'utilisateur appelé sache ce qui se passe. Certaines applications peuvent utiliser le support entrant comme une alerte.

3. Acceptation – exiger que l'utilisateur appelé prenne sa décision au démarrage. Demander à l'utilisateur de prendre une décision au démarrage sans alerter l'utilisateur sur le besoin de prendre une décision est généralement infaisable. Cela va avoir des implications sur de possibles options d'alerte qui sortent du domaine d'application de ce document.

4. Limiter les entrées/sorties (I/O) – Désactiver les haut-parleurs ou le microphone. Cela pourrait être utilisé pour convertir une session de supports bidirectionnels (très risqué, possible "punaise dans le téléphone") en session en entrée seulement unidirectionnelle (moins risqué, possibles "pourriels" ou "clôture", etc.) en attendant l'acceptation de l'utilisateur.

5. Politique -- les règles sur les autres facteurs, comme des listes noires et blanches fondées sur l'identité, interdisant l'acceptation sans alerte, etc.

Comme SIP et les travaux en rapport fournissent déjà plusieurs mécanismes (incluant l'authentification SIP par résumé [RFC3261], le mécanisme d'identité SIP [RFC4474], et le mécanisme SIP pour l'identité affirmée au sein des réseaux privés [RFC3325], dans les réseaux pour lesquels c'est convenable) pour établir l'identité de l'origine d'une demande, on présume qu'un mécanisme choisi de façon appropriée est disponible pour les UA qui mettent en œuvre les extensions décrites dans ce document. En bref, les UA qui mettent en œuvre ces extensions DOIVENT être équipés et DOIVENT appliquer un mécanisme d'identité de demande. L'analyse ci-dessous part de l'hypothèse que l'identité de l'envoyeur de chaque demande est soit connue, soit est connue pour être inconnue, et peut donc être considérée dans une politique en rapport. Manquer à satisfaire cette exigence d'identité ouvre la porte à une large gamme d'attaques ou exige une politique de fonctionnement assez stricte pour rendre ces extensions inutiles.

On a précédemment établi une distinction de classe entre flux de supports entrants et sortants, et on peut modéliser les flux bidirectionnels comme des sommes de "pires cas" des risques des deux autres classes. Étant donnée cette distinction, il semble raisonnable de donner des classes de politique séparées selon la direction pour :
1. Les flux de supports entrants.
2. Les flux de supports sortants.

Pour chaque classe de politique de direction, on peut diviser l'ensemble des identités de demande en trois classes :

1. Identités explicitement autorisées pour la classe.
2. Identités explicitement refusées pour la classe.
3. Identités pour lesquelles on a pas de politique explicite et sur lesquelles l'utilisateur doit prendre une décision.

Noter que toutes les combinaisons de politiques possibles de cette division ne sont pas généralement utiles. Spécifiquement, une politique de "support entrant refusé, support sortant accepté" équivaut à une attaque de "punaise dans le téléphone", et est interdite par la politique minimale du paragraphe 7.4, qui exclut comme c'est écrit tous les cas de "support sortant explicitement autorisé".

7.4 Exigence minimale de politique

Les agents d'utilisateur qui mettent en œuvre la présente spécification NE DEVRAIENT PAS établir une session fournissant des supports entrants sans acceptation explicite de l'utilisateur lorsque le demandeur est inconnu, ou est connu et n'a pas eu d'autorisation pour cette session. Cette exigence est destinée à empêcher les attaques de "diffusion de pourriels" lorsque des supports inattendus et non désirés sont exécutés sur un UAS.

Les agents d'utilisateur qui mettent en œuvre la présente spécification NE DOIVENT PAS établir une session fournissant des supports sortants ou bidirectionnels dont la source est l'agent d'utilisateur sans l'acceptation explicite de l'utilisateur. Les supports de rebouclage utilisés pour la vérification de connexité ne sont pas contraints par cette exigence. Cette exigence est destinée à assurer que cette extension ne peut pas être utilisée pour transformer un UAS en un microphone contrôlé à distance (ou "punaise") à l'insu de son utilisateur. Comme SIP permet qu'une session soit initialement établie avec des supports seulement entrants et transite ensuite (via re-INVITE ou UPDATE) vers une session sortante ou bidirectionnelle, appliquer cette politique exige une inspection de tous les états de dialogue dans l'UAS SIP. En d'autres termes, si une session a été initiée avec une réponse automatique, l'UAS NE DOIT PAS passer à un mode qui envoie des supports sortants sans acceptation explicite de l'utilisateur de l'UAS.

8. Considérations relatives à l'IANA

8.1 Enregistrement des champs d'en-tête

Le présent document définit de nouveaux champs d'en-tête SIP nommés "Answer-Mode" et "Priv-Answer-Mode".

Les lignes suivantes ont été ajoutées à la section "Champs d'en-tête" du registre des paramètres de SIP :

Nom d'en-tête	Forme compacte	Référence
Answer-Mode	-	[RFC5373]
Priv-Answer-Mode	-	[RFC5373]

8.2 Enregistrement des paramètres de champs d'en-tête

Le présent document définit des paramètres pour les champs d'en-tête définis dans le paragraphe précédant. Les champs d'en-tête "Answer-Mode" et "Priv-Answer-Mode" peuvent prendre les valeurs "Manual" ou "Auto".
Les rangées suivantes ont été ajoutées à la section "Paramètres de champ d'en-tête et valeurs de paramètres" du registre des paramètres de SIP :

Champ d'en-tête	Nom du paramètre	Valeurs prédéfinies	Référence
Answer-Mode	require	Non	[RFC5373] |
Priv-Answer-Mode	require	Non	[RFC5373] |

8.3. Enregistrement des étiquettes d'option SIP

Le présent document définit l'étiquette d'option SIP "answermode".
La rangée suivante a été ajoutée à la section "Étiquettes d'option" du registre des paramètres de SIP :

Nom	Description	Référence
answermode	Cette étiquette d'option est pour la prise en charge des extensions Answer-Mode et Priv-Answer-Mode utilisées pour négocier la réponse automatique ou manuelle à une demande.	[RFC5373]

9. Remerciements

Le présent document tire ses exigences et une grande partie de sa méthodologie du travail de "Open Mobile Alliance", et spécifiquement d'un document de Andrew Allen, Jan Holm, et Tom Hallin.

L'éditeur tient aussi à remercier de leurs contributions David Oran et d'autres qui ont argumenté sur la liste de diffusion du groupe de travail SIPPING et à la réunion OMA ad-hoc lors de l'IETF 62 que les idées sous-jacentes du document étaient en gros applicables à la communauté SIP, et que les concepts d'alerte et de réponse devraient être clairement précisés. De plus, la revue de la sécurité fournie par Sandy Murphy et la revue génerale de Suresh Krishnan ont été très utiles pour améliorer la qualité de ce document.

10. Références

10.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[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

[RFC3841] J. Rosenberg, H. Schulzrinne, P. Kyzivat, "Préférences de l'appelant pour le protocole d'initialisation de session (SIP)", août 2004. *(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. ; Remplacée par* RFC8224)

[RFC5234] D. Crocker, P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

10.2 Références pour information

[LOOPBACK] Hedayat, K., "An Extension to the Session Description Protocol (SDP) for Media Loopback", Travail en cours, août 2008.

[RFC3325] C. Jennings, J. Peterson et M. Watson, "Extensions privées au protocole d'initialisation de session (SIP) pour l'assertion d'identité au sein de réseaux de confiance", novembre 2002. *(Information ; MàJ par* RFC8217)

Adresse des auteurs

Dean Willis
Softarmor Systems
3100 Independence Pkwy #311-164
Plano, Texas 75075
USA
mél : dean.willis@softarmor.com

Andrew Allen
Research in Motion (RIM)
300 Knightsbridge Parkway, Suite 360
Lincolnshire, Illinois 60069
USA
mél : aallen@rim.com