Groupe de travail Réseau C. Newman, Innosoft
Request for Comments : 2595
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle juin 1999

Utilisation de TLS avec IMAP, POP3 et ACAP

Table des matières

1. Motivation....1
1.1 Conventions utilisées dans le document....2
2. Exigences de base d'interopérabilité et de sécurité....2
2.1 Exigences de suite de chiffrement....2
2.2 Exigences de sécurité du mode de fonctionnement confidentiel....2
2.3 Exigences sur le mot de passe en clair....2
2.4 Vérification de l'identité du serveur....2
2.5 Vérification de la politique de sécurité TLS....3
3. Extension IMAP STARTTLS....3
3.1 Commande STARTTLS....3
3.2 Capacité IMAP LOGINDISABLED....4
4. Extension POP3 STARTTLS....4
5. Extension ACAP STARTTLS....5
5.1 Commande STARTTLS....5
6. Mécanisme SASL PLAIN....5
7. Accès imaps et pop3s....6
8. Considérations relatives à l'IANA....7
9. Considérations sur la sécurité....7
9. Références....8
11. Adresse de l'auteur....9
A. Appendice -- Liste de vérification de conformité....9
Déclaration complète de droits de reproduction....9

1. Motivation

Le protocole TLS (anciennement appelé SSL) donne le moyen de sécuriser un protocole d'application contre l'altération et l'espionnage. L'option d'utiliser une telle sécurité est désirable pour IMAP, POP et ACAP à cause des attaques courantes d'espionnage et de capture de connexion [RFC1704]. Bien que les mécanismes évolués d'authentification SASL puissent fournir une version légère de ce service, TLS est complémentaire des mécanismes de simple authentification SASL ou des commandes déployées de mot de passe en clair.

De nombreux sites ont un fort investissement dans l'infrastructure d'authentification (par exemple, une large base de données de fonctions unidirectionnelles appliquées aux mots de passe d'utilisateur) de sorte qu'une couche de confidentialité qui n'est pas étroitement liée à l'authentification d'utilisateur peut protéger contre les attaques d'espionnage du réseau sans exiger une nouvelle infrastructure d'authentification et/ou forcer tous les utilisateurs à changer leur mot de passe. Reconnaissant que de tels sites désirent une authentification par simple mot de passe en combinaison avec le chiffrement TLS, la présente spécification définit le mécanisme SASL PLAIN à utiliser avec les protocoles à qui manque la commande d'authentification par simple mot de passe comme ACAP et SMTP. (Noter qu'il y a une autre RFC pour la commande STRARTTLS dans SMTP [RFC2487].)

Il y a un fort désir dans l'IETF d'éliminer la transmission de mots de passe en clair sur des canaux non chiffrés. Bien que SASL puisse être utilisé à cette fin, TLS procure un outil supplémentaire avec des caractéristiques de déploiement différentes. Un serveur qui prend en charge TLS avec des mots de passe simples et un mécanisme SASL de défi/réponse va probablement interopérer avec une large variété de clients sans recourir à des mots de passe en clair non chiffrés.

La commande STRARTTLS rectifie un certain nombre de problèmes de l'utilisation d'un accès séparé pour une variante de protocole "sécurisée". Certains d'eux sont mentionnés à la Section 7.

1.1 Conventions utilisées dans le document

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] pour indiquer les niveaux d'exigence.

Les termes relatifs à l'authentification sont définis dans "Authentification sur l'Internet" [RFC1704].

La syntaxe formelle est définie en utilisant l'ABNF [RFC2234].

Dans les exemples, "C :" et "S :" indiquent les lignes envoyées respectivement par le client et le serveur.

2. Exigences de base d'interopérabilité et de sécurité

Les exigences suivantes s'appliquent à toutes les mises en œuvre de l'extension STARTTLS pour IMAP, POP3 et ACAP.

2.1 Exigences de suite de chiffrement

La mise en œuvre de la suite de chiffrement TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA [RFC2246] est EXIGÉE. Ceci est important car cela assure que deux mises en œuvre conformes quelconques peuvent être configurées à interopérer.

Toutes les autres suites de chiffrement sont FACULTATIVES.

2.2 Exigences de sécurité du mode de fonctionnement confidentiel

Les clients et les serveurs DEVRAIENT avoir un mode de fonctionnement confidentiel qui refuse l'authentification tant que n'a pas été activée avec succès une couche de chiffrement (comme celle fournie par TLS) avant ou au moment de l'authentification et qui va terminer la connexion si cette couche de chiffrement est désactivée. Les mises en œuvre sont encouragées à être souples par rapport au minimum de force de chiffrement ou aux suites de chiffrement permises. Une approche minimaliste de cette recommandation serait un mode de fonctionnement où la suite de chiffrement TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA serait obligatoire avant de permettre l'authentification.

Les clients PEUVENT avoir un mode de fonctionnement qui n'utilise le chiffrement que quand il est annoncé par le serveur, mais où l'authentification continue néanmoins. Pour la rétro compatibilité, les serveurs DEVRAIENT avoir un mode de fonctionnement où seuls les mécanismes d'authentification requis par la spécification du protocole de base pertinent sont nécessaires pour réussir à s'authentifier.

2.3 Exigences sur le mot de passe en clair

Les clients et serveurs qui mettent en œuvre STARTTLS DOIVENT être configurables à refuser toutes les commandes ou mécanismes de connexion en clair (incluant les mécanismes sur la voie de la normalisation et ceux qui ne sont pas normalisés) à moins qu'une couche de chiffrement de force adéquate soit activée. Les serveurs qui permettent des établissements de connexion en clair non chiffrée DEVRAIENT pouvoir être configurés à refuser les établissements de connexion en clair, pour le serveur entier, et utilisateur par utilisateur.

2.4 Vérification de l'identité du serveur

Durant la négociation TLS, le client DOIT vérifier sa compréhension du nom d'utilisateur du serveur par rapport à l'identité du serveur présentée dans le message Certificat du serveur, afin d'empêcher les attaques par interposition. La confrontation est effectuée selon les règles suivantes :

- Le client DOIT utiliser le nom d'utilisateur que le serveur a utilisé pour ouvrir la connexion comme la valeur à comparer au nom de serveur exprimé dans le certificat du serveur. Le client NE DOIT utiliser aucune forme de nom d'utilisateur du serveur déduite d'une source distante non sûre (par exemple, une recherche non sécurisée sur le DNS). La canonisation du CNAME n'est pas faite.

- Si une extension subjectAltName de type dNSName est présente dans le certificat, elle DEVRAIT être utilisée comme source de l'identité du serveur.

- La confrontation est insensible à la casse.

- Un caractère générique "*" PEUT être utilisé pour les composants les plus à gauche du nom dans le certificat. Par exemple, *.exemple.com va correspondre à a.exemple.com, foo.exemple.com, etc. mais ne correspondrait pas à exemple.com ou foo.bar.exemple.com. *.*.exemple.com correspondrait pour foo.bar.exemple.com mais pas pour foo.exemple.com.

- Si le certificat contient plusieurs noms (par exemple plus d'un champ dNSName) une correspondance d'un de ces champs est considérée comme acceptable.

Si la confrontation échoue, le client DEVRAIT soit demander une confirmation explicite de l'utilisateur, soit terminer la connexion et indiquer que l'identité du serveur est suspecte.

2.5 Vérification de la politique de sécurité TLS

Le client et le serveur DOIVENT tous deux vérifier le résultat de la commande STRARTTLS et de la négociation TLS qui s'ensuit pour voir si une authentification ou confidentialité acceptable a été réalisée. Ignorer cette étape invalide complètement l'utilisation de TLS pour la sécurité. La décision que l'authentification ou la confidentialité est acceptable est prise en local, et dépend de la mise en œuvre, et sort du domaine d'application du présent document.

3. Extension IMAP STARTTLS

Quand l'extension TLS est présente dans IMAP, "STARTTLS" est mentionné comme capacité en réponse à la commande CAPABILITY. Cette extension ajoute une seule commande, "STARTTLS" au protocole IMAP qui est utilisé pour commencer la négociation TLS.

3.1 Commande STARTTLS

Arguments : aucun
Réponses : pas de réponse spécifique pour cette commande
Résultat : OK - commencer la négociation TLS
BAD - commande inconnue ou arguments invalides

Une négociation TLS commence immédiatement après le CRLF à la fin de la réponse OK étiquetée provenant du serveur. Une fois qu'un client a produit une commande STRARTTLS, il NE DOIT PAS produire d'autres commandes tant qu'il n'a pas vu une réponse du serveur et que la négociation TLS n'est pas achevée.

La commande STRARTTLS n'est valide que dans l'état non authentifié. Le serveur reste dans l'état non authentifié, même si les accréditifs du client sont fournis durant la négociation TLS. Le mécanisme SASL EXTERNAL [RFC2222] PEUT être utilisé pour authentifier une fois que les accréditifs du client TLS ont bien été échangés, mais les serveurs qui prennent en charge la commande STRARTTLS ne sont pas obligés de prendre en charge le mécanisme EXTERNAL.

Une fois que TLS a commencé, le client DOIT éliminer les informations d'antémémoire sur les capacités du serveur et DEVRAIT produire à nouveau la commande CAPABILITY. Ceci est nécessaire pour la protection contre les attaques par interposition qui altèrent la liste des capacités avant le STARTTLS. Le serveur PEUT annoncer des capacités différentes après le STARTTLS.

La syntaxe formelle pour IMAP est amendée comme suit :

command_any =/ "STARTTLS"

Exemple :
C : a001 CAPABILITY
S : * CAPABILITY IMAP4rev1 STARTTLS LOGINDISABLED
S : a001 OK CAPABILITY achevé
C : a002 STARTTLS
S : a002 OK commencer la négociation TLS maintenant
<négociation TLS, les autres commandes sont sous la couche TLS>
C : a003 CAPABILITY
S : * CAPABILITY IMAP4rev1 AUTH=EXTERNAL
S : a003 OK CAPABILITY achevé
C : a004 LOGIN mot de passe de Claude
S : a004 OK LOGIN achevé

3.2 Capacité IMAP LOGINDISABLED

La spécification actuelle du protocole IMAP [RFC2060] exige la mise en œuvre de la commande LOGIN qui utilise des mots de passe en clair. De nombreux sites peuvent choisir de désactiver cette commande sauf si le chiffrement est activé pour des raisons de sécurité. Un serveur IMAP PEUT annoncer que la commande LOGIN est désactivée en incluant la capacité LOGINDISABLED dans la réponse de capacités. Un tel serveur va répondre avec une réponse "NO" étiquetée à toute tentative d'utilisation de la commande LOGIN.

Un serveur IMAP qui met en œuvre STARTTLS DOIT mettre en œuvre la prise en charge de la capacité LOGINDISABLED sur les connexions non chiffrées.

Un client IMAP qui se conforme à la présente spécification NE DOIT PAS produire la commande LOGIN si cette capacité est présente.

Cette capacité est utile pour empêcher les clients conformes à la présente spécification d'envoyer un mot de passe non chiffré dans un environnement soumis à des attaques passives. Elle n'a pas d'impact sur un environnement soumis à des attaques actives car un attaquant interposé peut supprimer cette capacité. Donc cela ne libère pas les clients de la nécessité de suivre la recommandation de mode confidentiel du paragraphe 2.2.

Les serveurs qui annoncent cette capacité vont échouer à interopérer avec de nombreux clients IMAP conformes existants et seront dans l'incapacité d'empêcher ces clients de divulguer le mot de passe de l'utilisateur.

4. Extension POP3 STARTTLS

L'extension POP3 STARTTLS ajoute la commande STLS aux serveurs POP3. Si elle est mise en œuvre, le mécanisme d'extension POP3 [RFC2449] DOIT aussi être mis en œuvre pour éviter que le client ait besoin d'essayer plusieurs commandes. Le nom de capacité "STLS" indique que cette commande est présente et permise dans l'état actuel.

STLS
Arguments : aucun
Restrictions : seulement permise dans l'état AUTHORIZATION.
Discussion : une négociation TLS commence immédiatement après le CRLF à la fin de la réponse +OK provenant du serveur. Une réponse -ERR PEUT résulter si une couche de sécurité est déjà active. Une fois qu'un client a produit une commande STLS, il NE DOIT PAS produire d'autres commandes jusqu'à ce qu'il voit la réponse d'un serveur et que la négociation TLS soit achevée.

La commande STLS n'est permise que dans l'état AUTHORIZATION et le serveur reste dans l'état AUTHORIZATION, même si les accréditifs du client sont fournis durant la négociation TLS. La commande AUTH [RFC1734] avec le mécanisme EXTERNAL [RFC2222] PEUT être utilisée pour l'authentification une fois que les accréditifs du client TLS sont bien échangés, mais les serveurs qui prennent en charge la commande STLS ne sont pas obligés de prendre en charge le mécanisme EXTERNAL.

Une fois que TLS a démarré, le client DOIT éliminer les informations d'antémémoire sur les capacités du serveur et DEVRAIT produire une nouvelle commande CAPA. Ceci est nécessaire pour protéger contre les attaques par interposition qui altèrent la liste de capacités avant le STLS. Le serveur PEUT annoncer des capacités différentes après le STLS.

Réponses possibles : +OK -ERR

Exemples :
C : STLS
S : +OK commencer la négociation TLS
<négociation TLS, les autres commandes sont sous la couche TLS>
...
C : STLS
S : -ERR Commande non permise quand TLS est actif.

5. Extension ACAP STARTTLS

Quand l'extension TLS est présente dans ACAP, "STARTTLS" figure sur la liste comme capacité dans l'accueil ACAP. Aucun argument de cette capacité n'est défini pour l'instant. Cette extension ajoute une seule commande, "STARTTLS" au protocole ACAP qui est utilisé pour commencer une négociation TLS.

5.1 Commande STARTTLS

Arguments : aucun
Réponses : aucune réponse spécifique pour cette commande.
Résultat : OK - commencer la négociation TLS
BAD - commande inconnue ou arguments invalides.

Une négociation TLS commence immédiatement après le CRLF à la fin de la réponse étiquetée OK provenant du serveur. Une fois qu'un client a produit une commande STRARTTLS, il NE DOIT PAS produire d'autre commande jusqu'à ce qu'il ait vu une réponse du serveur et que la négociation TLS soit achevée.

La commande STRARTTLS n'est valide que dans l'état non authentifié. Le serveur reste dans l'état non authentifié, même si les accréditifs du client sont fournis durant la négociation TLS. Le mécanisme SASL EXTERNAL [RFC2222] PEUT être utilisé pour authentifier une fois que les accréditifs du client TLS ont été bien échangés, mais les serveurs qui prennent en charge la commande STRARTTLS ne sont pas obligés de prendre en charge le mécanisme EXTERNAL.

Après l'établissement de la couche TLS, le serveur DOIT produire à nouveau un accueil ACAP non étiqueté. C'est nécessaire pour protéger contre les attaques par interposition qui altèrent la liste de capacités avant le STARTTLS. Le client DOIT éliminer les informations de capacité de l'antémémoire et les remplacer par les informations provenant du nouvel accueil ACAP. Le serveur PEUT annoncer des capacités différentes après le STARTTLS.

La syntaxe formelle pour ACAP est amendée comme suit :

command_any =/ "STARTTLS"

Exemple :
S : * ACAP (SASL "CRAM-MD5") (STARTTLS)
C : a002 STARTTLS
S : a002 OK "Commencer maintenant la négociation TLS"
<négociation TLS, les autres commandes sont sous la couche TLS>
S : * ACAP (SASL "CRAM-MD5" "PLAIN" "EXTERNAL")

6. Mécanisme SASL PLAIN

Les mots de passe en clair sont simples, ils interopèrent avec la plupart des bases de données d'authentification des systèmes d'exploitation existants, et sont utiles pour une transition en douceur à un mécanisme d'authentification plus sûr fondé sur le mot de passe. L'inconvénient est qu'il est inacceptable de les utiliser sur une connexion réseau qui n'est pas chiffrée.

Cela définit le mécanisme SASL "PLAIN" à utiliser avec ACAP et d'autres protocoles sans commande d'amorçage en clair. Le mécanisme SASL PLAIN NE DOIT PAS être annoncé ou utilisé sans une forte couche de chiffrement (comme celle fournie par TLS) active sauf si des problèmes de rétro compatibilité dictent une autre conduite.

Le mécanisme consiste en un seul message du client au serveur. Le client envoie l'identité d'autorisation (l'identité pour se connecter comme) suivi par un caractère US-ASCII NUL, suivi par l'identité d'authentification (identité dont le mot de passe sera utilisé) suivi par un caractère US-ASCII NUL, suivi par le mot de passe en clair. Le client peut laisser l'identité d'autorisation vide pour indiquer qu'elle est la même que l'identité d'authentification.

Le serveur va vérifier l'identité d'authentification et le mot de passe avec la base de données d'authentification du système et vérifier que les accréditifs d'authentification permettent au client de se connecter comme identité d'autorisation. Si les deux étapes réussissent, l'utilisateur est connecté.

Le serveur PEUT aussi utiliser le mot de passe pour initialiser toute nouvelle base de données d'authentification, comme une qui conviendrait pour CRAM-MD5 [RFC2195].

Les caractères non US-ASCII sont permis pour autant qu'ils soient représentés en UTF-8 [RFC2279]. L'utilisation de caractères non visibles ou de caractères qu'un utilisateur ne pourrait pas entrer sur certains claviers est déconseillée.

La grammaire formelle en ABNF [RFC2234] pour le message du client est la suivante :

message = [identité d'autorisation] NUL identité d'authentification NUL mot de passe
identité d'authentification = 1*UTF8-SAFE ; DOIT accepter jusqu'à 255 octets
identité d'autorisation = 1*UTF8-SAFE ; DOIT accepter jusqu'à 255 octets
mot de passe = 1*UTF8-SAFE ; DOIT accepter jusqu'à 255 octets
NUL = %x00
UTF8-SAFE = %x01-09 / %x0B-0C / %x0E-7F / UTF8-2 / UTF8-3 / UTF8-4 / UTF8-5 / UTF8-6
UTF8-1 = %x80-BF
UTF8-2 = %xC0-DF UTF8-1
UTF8-3 = %xE0-EF 2UTF8-1
UTF8-4 = %xF0-F7 3UTF8-1
UTF8-5 = %xF8-FB 4UTF8-1
UTF8-6 = %xFC-FD 5UTF8-1

Voici un exemple de la façon dont cela peut être utilisé pour initialiser une base de données d'authentification CRAM-MD5 pour ACAP:

Exemple :
S : * ACAP (SASL "CRAM-MD5") (STARTTLS)
C : a001 AUTHENTICATE "CRAM-MD5"
S : + "<1896.697170952@postoffice.reston.mci.net>"
C : "tim b913a602c7eda7a495b4e6e7334d3890"
S : a001 NO (TRANSITION-NEEDED) "Prière de changer votre mot de passe, ou d'utiliser TLS pour se connecter"
C : a002 STARTTLS
S : a002 OK "Commencer maintenant la négociation TLS"
<négociation TLS, les commandes suivantes sont sous la couche TLS>
S : * ACAP (SASL "CRAM-MD5" "PLAIN" "EXTERNAL")
C : a003 AUTHENTICATE "PLAIN" {21+}
C : <NUL>tim<NUL>tanstaaftanstaaf
S : a003 OK CRAM-MD5 mot de passe initialisé

Note : dans cet exemple, <NUL> représente un seul octet ASCII NUL.

7. Accès imaps et pop3s

Des accès "imaps" et "pop3s" séparés ont été enregistrés pour être utilisés avec SSL. L'utilisation de ces accès est déconseillée et on recommande plutôt l'utilisation des commandes STARTTLS ou STLS.

Un certain nombre de problèmes ont été observés avec les accès séparés pour des variantes "sûres" de protocoles. On essaye ici de les énumérer.

- Les accès séparés conduisent à un schéma d'URL séparé qui fait intrusion de façon inappropriée dans l'interface de l'utilisateur. Par exemple, de nombreuses pages de la Toile utilisent un langage du genre "cliquer ici si votre navigateur prend en charge SSL". C'est une décision que le navigateur est souvent plus capable de prendre que l'utilisateur.

- Les accès séparés impliquent un modèle de "sûr" ou "non sûr". Cela peut être trompeur de beaucoup de façons. D'abord, l'accès "sûr" peut n'être en fait pas acceptablement sûr car une suite de chiffrement dégradée pour l'exportation peut être utilisée. Cela peut tromper les utilisateurs qui vont éprouver à tort un sentiment de sécurité. Ensuite, l'accès normal peut en fait être sécurisé par l'usage d'un mécanisme SASL qui comporte une couche de sécurité. Donc, la distinction d'accès séparé rend le sujet complexe de la politique de sécurité encore plus confus. Un résultat courant de cette confusion est que les administrateurs de pare-feu sont souvent amenés à tort à permettre l'accès "sûr" et à bloquer l'accès standard. Ce peut être un mauvais choix étant donné que l'utilisation courante de SSL avec une couche de chiffrement à clé de 40 bits et une authentification par mot de passe en clair est moins sûre que de forts mécanismes SASL comme GSSAPI avec Kerberos 5.

- L'utilisation d'accès séparés pour SSL a amené des clients à mettre en œuvre seulement deux politiques de sécurité: utiliser SSL ou ne pas utiliser SSL. La politique de sécurité désirable "utiliser TLS quand il est disponible" serait absurde avec le modèle d'accès séparé, mais elle est simple avec STARTTLS.

- Les numéros d'accès sont une ressource limitée. Bien que ce ne soit pas encore la disette, il ne serait pas sage d'établir un précédent qui pourrait doubler (ou pire) leur vitesse de consommation.

8. Considérations relatives à l'IANA

Ceci constitue l'enregistrement des capacités IMAP "STARTTLS" et "LOGINDISABLED" comme exigé par le paragraphe 7.2.1 de la [RFC2060].

L'enregistrement de la capacité POP3 "STLS" est le suivant :
Étiquette CAPA : STLS
Arguments : aucun
Commande ajoutée : STLS
Commandes standard affectées : peut activer USER/PASS comme effet collatéral. La commande CAPA DEVRAIT être produite à nouveau après un bon achèvement.
États annoncés/valides : seulement l'état AUTHORIZATION.
Spécification de référence : le présent mémoire.

L'enregistrement pour la capacité ACAP "STARTTLS" est le suivant :
Nom de capacité : STARTTLS
Mot clé : STARTTLS
Arguments : aucun
Spécification publiée : le présent mémoire.
Adresse personnelle et de messagerie pour informations : voir le paragraphe "adresse de l'auteur" ci-dessous.

L'enregistrement pour le mécanisme SASL PLAIN est le suivant :
Nom du mécanisme SASL : PLAIN
Considérations sur la sécurité : voir la Section 9 du présent mémoire.
Spécification publiée : le présent mémoire.
Adresse personnelle et de messagerie pour informations : voir le paragraphe "adresse de l'auteur" ci-dessous.
Utilisation prévue : COMMUNE
Auteur/contrôleur des changements : voir le paragraphe "adresse de l'auteur" ci-dessous.

9. Considérations sur la sécurité

TLS ne fournit de protection que pour les données envoyées sur une connexion réseau. Les messages transférés sur IMAP ou POP3 sont toujours disponibles aux administrateurs de serveur et sont généralement soumis à l'espionnage, l'altération et la falsification lors de leur transmission par SMTP ou NNTP. TLS n'est pas un substitut d'un mécanisme de sécurité de message de bout en bout utilisant la sécurité de MIME multi parties [RFC1847].

Les attaques par interposition peuvent supprimer STARTTLS de la liste de capacités ou générer une réponse d'échec à la commande STRARTTLS. Afin de détecter de telles attaques, les clients DEVRAIENT avertir l'utilisateur quand la confidentialité de la session n'est pas activée et/ou est configurable à refuser de poursuivre sans un niveau acceptable de sécurité.

Un attaquant interposé peut toujours causer une négociation dégradée au plus faible mécanisme d'authentification ou suite de chiffrement disponible. Pour cette raison, les mises en œuvre DEVRAIENT être configurables à refuser les mécanismes ou suites de chiffrement faibles.

Toutes les interactions de protocole avant la prise de contact TLS sont effectuées en clair et peuvent être modifiées par un attaquant interposé. Pour cette raison, les clients DOIVENT éliminer les informations en antémémoire sur les capacités du serveur annoncées avant le début de la prise de contact TLS.

Les clients sont encouragés à indiquer clairement quand le niveau de chiffrement activé est réputé vulnérable à une attaque utilisant un matériel moderne (comme des clés de chiffrement avec 56 bits d'entropie ou moins).

La capacité LOGINDISABLED IMAP (discutée au paragraphe 3.2) réduit seulement le potentiel d'attaques passives, elle ne fournit aucune protection contre les attaques actives. Le client conserve la responsabilité d'éviter d'envoyer un mot de passe sur un canal vulnérable.

Le mécanisme PLAIN s'appuie sur la couche de chiffrement TLS pour sa sécurité. Quand il est utilisé sans TLS, il est vulnérable à une attaque courante d'espionnage du réseau. Donc, PLAIN NE DOIT PAS être annoncé ou utilisé sans l'activation d'une couche de chiffrement TLS convenable à moins que des soucis de rétro compatibilité l'imposent.

Quand le mécanisme PLAIN est utilisé, le serveur gagne la capacité de se faire passer pour l'utilisateur de tous les services avec le même mot de passe sans considération de tout chiffrement fourni par TLS ou autre mécanisme de confidentialité du réseau. Bien que de nombreux autres mécanismes d'authentification aient des faiblesses similaires, des mécanismes SASL plus forts comme Kerberos traitent ce problème. Les clients sont encouragés à avoir un mode de fonctionnement où tous les mécanismes qui vont probablement révéler le mot de passe de l'utilisateur au serveur sont désactivés.

Les considérations de sécurité pour TLS s'appliquent à STARTTLS et les considérations de sécurité pour SASL s'appliquent au mécanisme PLAIN. Des exigences de sécurité supplémentaires sont discutées dans la Section 2.

9. Références

[RFC1704] N. Haller et R. Atkinson, "Authentification sur l'Internet", octobre 1994. *(Information)*

[RFC1734] J. Myers, "Commande POP3 AUTHentification", décembre 1994. *(P.S., remplacée par la* RFC5034)

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, 2449, 8314) (STD0053)

[RFC2060] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", décembre 1996. *(Remplace* RFC1730) (*Obsolète, voir* RFC3501) *(P.S.)*

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

[RFC2195] J. Klensin et autres, "Extension IMAP/POP AUTHorize pour mise au défi/réponse simple", septembre 1997. *(P.S.)*

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2244] C. Newman, J. G. Myers,"ACAP – Protocole d'accès à la configuration d'application", novembre 1997. *(P.S.)*

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[RFC2279] F. Yergeau, "UTF-8, un format de transformation de la norme ISO 10646", janvier 1998. (*Obsolète, voir* RFC3629) *(D.S.)*

[RFC2449] R. Gellens, C. Newman, L. Lundblade, "Mécanisme d'extension de POP3", novembre 1998. (*MàJ par* RFC5034) *(P.S.)*

[RFC2487] P. Hoffman, "Extension de service SMTP pour SMTP sécurisé sur TLS", janvier 1999. (*Obsolète, voir* RFC3207) *(P.S.)*

11. Adresse de l'auteur

Chris Newman
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790
USA
mél : chris.newman@innosoft.com

A. Appendice -- Liste de vérification de conformité

Une mise en œuvre n'est pas conforme si elle échoue à satisfaire une ou plusieurs des exigences DOIT pour les protocoles qu'elle met en œuvre. Une mise en œuvre qui satisfait toutes les exigences DOIT et DEVRAIT pour ses protocoles est dite être "inconditionnellement conforme" ; celle qui satisfait toutes les exigences DOIT mais pas toutes les exigences DEVRAIT pour ses protocoles est dite être "conditionnellement conforme".

Règles	**Paragraphe**
Suite de chiffrement de mise en œuvre obligatoire	2.1
DEVRAIT avoir un mode où le chiffrement est exigé	2.2
Le serveur DEVRAIT avoir un mode où TLS 'est pas exigé	2.2
DOIT être configurable à refuser toute commande ou mécanisme de connexion en clair	2.3
Le serveur DEVRAIT être configurable à refuser les commandes de connexion en clair pour tout le serveur et sur la base de l'utilisateur	2.3
Le client DOIT vérifier l'identité du serveur	2.4
Le client DOIT utiliser le nom d'utilisateur utilisé pour ouvrir la connexion	2.4
Le client NE DOIT PAS utiliser le nom d'utilisateur pour les recherches distantes non sûres	2.4
Le client DEVRAIT prendre en charge le subjectAltName de type dNSName	2.4
Le client DEVRAIT demander confirmation ou terminer sur échec	2.4
DOIT vérifier le résultat de STARTTLS pour une confidentialité acceptable	2.5
Le client NE DOIT PAS produire de commande après STARTTLS jusqu'à la réponse du serveur et la fin de la négociation	3.1, 4, 5.1
Le client DOIT éliminer les informations en antémémoire	3.1, 4, 5.1, 9
Le client DEVRAIT produire une nouvelle commande CAPABILITY/CAPA	3.1, 4
Le serveur IMAP avec STARTTLS DOIT mettre en œuvre LOGINDISABLED	3.2
Le client IMAP NE DOIT PAS produire de LOGIN si LOGINDISABLED	3.2
Le serveur POP DOIT mettre en œuvre les extensions POP3	4
Le serveur ACAP DOIT produire un nouvel accueil ACAP	5.1
Le client DEVRAIT avertir que la confidentialité de session n'est pas active et/ou refuser de continuer sans un niveau de sécurité acceptable	9
DEVRAIT être configurable à refuser les mécanismes ou suites de chiffrement faibles	9

Le mécanisme PLAIN est une partie facultative de cette spécification. Cependant si elle est mise en œuvre, les règles suivantes s'appliquent :

Règles	**Section**
NE DOIT PAS utiliser PLAIN sauf si un fort chiffrement est activé ou si la rétro compatibilité l'impose	6, 9
DOIT utiliser le codage UTF-8 pour les caractères dans PLAIN	6

Déclaration complète de droits de reproduction

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org .

Remerciement

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