Groupe de travail Réseau
Request for Comments : 2712
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

A. Medvinsky, Excite
M. Hur, CyberSafe Corporation
octobre 1999

Ajout de suites de chiffrement Kerberos à la sécurité de la couche Transport (TLS)

Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet 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 "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Note de l'IESG

Les suites de chiffrement de 40 bits définies dans le présent mémoire ne sont incluses que pour documenter le fait que ces suites de chiffrement ont déjà été allouées. Les suites de chiffrement de 40 bits ont été conçues pour se conformer à US-centric, et à des restrictions à l'exportation, maintenant obsolètes. Elles n'ont jamais été sûres, et de nos jours, sont inadéquates même pour des applications insouciantes de la sécurité. La mise en œuvre et l'utilisation des suites de chiffrement à 40 bits définies dans le présent document, et ailleurs, est fortement déconseillée.

1. Résumé

Le présent document propose l'ajout de nouvelles suites de chiffrement au protocole TLS [RFC2246] pour prendre en charge l'authentification fondée sur Kerberos. Les accréditifs Kerberos sont utilisés pour réaliser l'authentification mutuelle et pour établir un secret maître qui est ensuite utilisé pour sécuriser la communication client-serveur.

2. Introduction

La souplesse est une des principales forces du protocole TLS. Clients et serveurs peuvent négocier les suites de chiffrement pour satisfaire des politiques administratives et de sécurité spécifiques. Cependant, aujourd'hui, l'authentification dans TLS est limitée aux seules solutions à clé publique. Il en résulte que TLS ne prend pas pleinement en charge les organisations avec des déploiements de sécurité hétérogènes qui incluent des systèmes d'authentification fondés sur la cryptographie symétrique. Kerberos, développé à l'origine au MIT, se fonde sur un standard ouvert [RFC1510] et est le système d'authentification à clé symétrique le plus largement déployé. Le présent document propose une nouvelle option pour négocier l'authentification Kerberos au sein du cadre TLS. Cela réalise l'authentification mutuelle et l'établissement d'un secret maître qui utilise les accréditifs Kerberos. Les changements proposés sont minimum et, en fait, pas différents de l'ajout d'un nouvel algorithme de clé publique au cadre TLS.

3. Option d'authentification Kerberos dans TLS

La présente section décrit l'ajout de l'option d'authentification Kerberos au protocole TLS. Tout au long du présent document, on se réfère à la prise de contact SSL de base montrée à la Figure 1. Pour des détails sur la prise de contact TLS, se reporter à la [RFC2246].

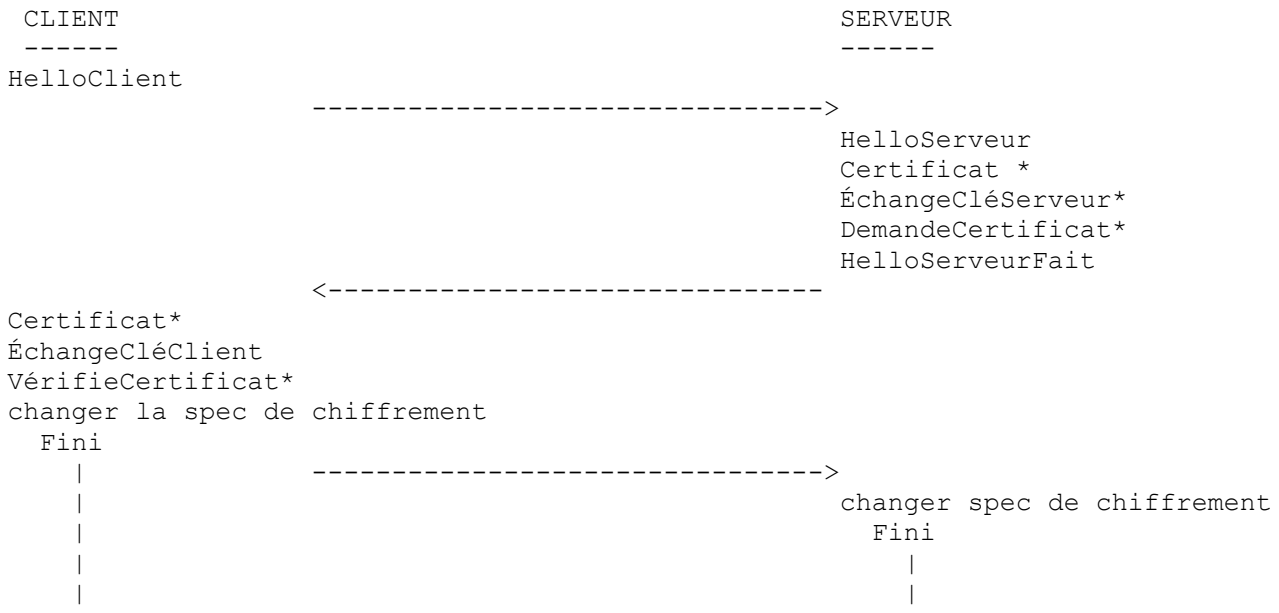

Figure 1 : Protocole TLS

Tous les messages suivis d'une étoile sont facultatifs. Note : Cette figure est tirés d'un document de l'IETF [RFC2246].

Le contexte de sécurité TLS est négocié dans les messages hello du client et du serveur. Par exemple : TLS_RSA_WITH_RC4_MD5 signifie que l'authentification initiale sera faite en utilisant l'algorithme à clé publique RSA, que RC4 sera utilisé pour la clé de session, et que les MAC seront fondés sur l'algorithme MD5. Donc, pour faciliter l'option d'authentification Kerberos, on doit commencer par définir de nouvelles suites de chiffrement incluant (sans s'y limiter) :

```
CipherSuite   TLS_KRB5_WITH_DES_CBC_SHA              = { 0x00,0x1E };
CipherSuite   TLS_KRB5_WITH_3DES_EDE_CBC_SHA         = { 0x00,0x1F };
CipherSuite   TLS_KRB5_WITH_RC4_128_SHA              = { 0x00,0x20 };
CipherSuite   TLS_KRB5_WITH_IDEA_CBC_SHA             = { 0x00,0x21 };
CipherSuite   TLS_KRB5_WITH_DES_CBC_MD5              = { 0x00,0x22 };
CipherSuite   TLS_KRB5_WITH_3DES_EDE_CBC_MD5         = { 0x00,0x23 };
CipherSuite   TLS_KRB5_WITH_RC4_128_MD5              = { 0x00,0x24 };
CipherSuite   TLS_KRB5_WITH_IDEA_CBC_MD5             = { 0x00,0x25 };
CipherSuite   TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA    = { 0x00,0x26 };
CipherSuite   TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA    = { 0x00,0x27 };
CipherSuite   TLS_KRB5_EXPORT_WITH_RC4_40_SHA        = { 0x00,0x28 };
CipherSuite   TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5    = { 0x00,0x29 };
CipherSuite   TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5    = { 0x00,0x2A };
CipherSuite   TLS_KRB5_EXPORT_WITH_RC4_40_MD5        = { 0x00,0x2B };
```

Pour établir un contexte de sécurité fondé sur Kerberos, une ou plusieurs des suites de chiffrement ci-dessus doivent être spécifiées dans le message hello du client. Si le serveur TLS prend en charge l'option d'authentification Kerberos, le message hello de serveur, envoyé au client, va confirmer la suite de chiffrement Kerberos choisie par le serveur. Le certificat du serveur, la demande de certificat du client, et l'échange de clé de serveur montrés à la Figure 1 seront omis car l'authentification et l'établissement d'un secret maître seront faits en utilisant les accréditifs Kerberos du client pour le serveur TLS. Le certificat du client sera omis pour la même raison. Noter que ces messages sont spécifiés comme facultatifs dans le protocole TLS ; donc, il est permis de les omettre.

L'option Kerberos doit être ajoutée au message ÉchangeCléClient comme le montre la Figure 2.

```
struct
{
  select (KeyExchangeAlgorithm)
  {
    case krb5:           KerberosWrapper;                /* nouvel ajout */
    case rsa:            EncryptedPreMasterSecret;
    case diffie_hellman: ClientDiffieHellmanPublic;
```

```
    } Exchange_keys;

} ÉchangeCléClient;

struct
{
    opaque Ticket;
    opaque authenticator;                          /* facultatif */
    opaque EncryptedPreMasterSecret;               /* chiffré avec la clé de session qui est scellée dans le ticket */
} KerberosWrapper;                                 /* new addition */
```

Figure 2 : Option Kerberos dans l'échange de clé de client

Pour utiliser l'option d'authentification Kerberos, le client TLS doit obtenir un ticket de service pour le serveur TLS. Dans TLS, le message ÉchangeCléClient est utilisé pour passer un secret aléatoire pré maître de 48 octets au serveur.

Le client et le serveur utilisent alors le secret pré maître pour déduire indépendamment le secret maître, qui à son tour est utilisé pour générer les clés de session et pour les calculs de MAC. Donc, si l'option Kerberos est choisie, la structure de secret pré maître est la même que celle utilisée dans le cas RSA ; elle est chiffrée sous la clé de session Kerberos et envoyée au serveur TLS avec les accréditifs Kerberos (voir la Figure 2). Le ticket et l'authentificateur sont codés selon la RFC1510 (codage ASN.1). Une fois que le message ÉchangeCléClient a été reçu, la clé secrète du serveur est utilisée pour désenvelopper les accréditifs et extraire le secret pré maître.

Noter qu'un authentifiant Kerberos n'est pas exigé, car le secret maître déduit par le client et le serveur ont pour germe une valeur aléatoire passée dans le message hello du serveur, déjouant ainsi les attaques en répétition. Cependant, l'authentifiant peut quand même se révéler utile pour passer les informations d'autorisation et il lui est donc alloué un champ facultatif (voir la Figure 2).

Enfin, le client et le serveur échangent les messages finis pour achever la prise de contact. À ce point, on a réalisé ce qui suit :

1) un secret maître, utilisé pour protéger toute la communication suivante, est établi de façon sûre,
2) l'authentification mutuelle client-serveur est réalisée, car le serveur TLS prouve qu'il a connaissance du secret maître dans le message fini.

Noter que l'option Kerberos se fait sans interruption, sans ajouter de nouveau message.

4. Conventions de désignation

Pour obtenir un ticket de service approprié, le client TLS doit déterminer le nom principal du serveur TLS. La convention de désignation de service Kerberos est utilisée à cette fin comme suit :

hôte/NomDeMachine@Domaine

où :

- le littéral, "hôte", suit la convention Kerberos lorsque il n'est pas concerné par le domaine de protection sur une machine particulière,
- "NomDeMachine" est l'instance particulière du service,
- le "Domaine" Kerberos est le nom de domaine de la machine.

5. Résumé

L'option d'authentification Kerberos proposée est ajoutée exactement de la même manière que le serait un nouvel algorithme de clé publique à TLS. De plus, elle établit le secret maître exactement de la même manière.

6. Considérations pour la sécurité

Les suites de chiffrement Kerberos sont soumises aux mêmes considérations de sécurité que le protocole TLS. De plus, tout comme une mise en œuvre de clé publique doit faire attention à protéger la clé privée (par exemple, le PIN pour une carte à mémoire) une mise en œuvre Kerberos doit faire attention à protéger le secret de longue durée qui est partagé entre le principal et le KDC. En particulier, un mot de passe faible peut subir une attaque de dictionnaire. Afin de renforcer

l'authentification initiale auprès d'un KDC, une mise en œuvre peut choisir d'utiliser une authentification secondaire via une carte à jeton, ou on peut utiliser l'authentification initiale auprès du KDC fondée sur le chiffrement à clé publique (appelé couramment PKINIT - un produit du groupe de travail Common Authentication Technology de l'IETF).

7. Remerciements

Merci à Clifford Neuman pour ses précieux commentaires sur les versions précédentes de ce document.

8. Références

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

[RFC1510] J. Kohl et C. Neuman, "Service Kerberos d'authentification de réseau (v5)", septembre 1993. *(Obsolète, voir RFC6649)*

9. Adresse des auteurs

Ari Medvinsky
Excite
555 Broadway
Redwood City, CA 94063
téléphone : +1 650 569 2119
mél : amedvins@excitecorp.com
http://www.excite.com

Matthew Hur
CyberSafe Corporation
1605 NW Sammamish Road
Issaquah WA 98027-5378
téléphone : +1 425 391 6000
mél : matt.hur@cybersafe.com
http://www.cybersafe.com

10. Déclaration complète de droits de reproduction

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