Groupe de travail Réseau
Request for Comments : 4107
BCP 107
Catégorie : Bonnes pratiques actuelles

S. Bellovin, Columbia University
R. Housley, Vigil Security
juin 2005
Traduction Claude Brière de L'Isle

Lignes directrices pour la gestion des clés de chiffrement

Résumé
La question se pose souvent de savoir si un certain système de sécurité exige une forme de gestion de clé automatique, ou si le chiffrement manuel est suffisant. Le présent mémoire apporte des lignes directrices pour prendre une telle décision. Lorsque des mécanismes de chiffrement symétriques sont utilisés dans un protocole, la présomption est que la gestion automatique de clé est généralement nécessaire, mais pas toujours. Si le chiffrement manuel est proposé, la charge de prouver que la gestion automatique de clé n'est pas exigée incombe à celui qui propose.

Table of Contents

1. Introduction

La question se pose souvent de savoir si un certain système de sécurité exige ou non une forme de gestion de clé automatique, ou si le chiffrement manuel est suffisant.

Il n'y a pas une réponse unique à cette question ; cela dépend des circonstances. En général, la gestion automatique de clés DEVRAIT être utilisée. Occasionnellement, il est raisonnable de s'appuyer sur la gestion manuelle des clés. On propose quelques lignes directrices pour trancher cette question.

D'un autre côté, s'appuyer sur la gestion manuelle des clés présente des inconvénients significatifs, et on souligne les problèmes de sécurité qui justifient la préférence pour la gestion automatique. Cependant, il y a des situations dans lesquelles la gestion manuelle des clés est acceptable.

1.1 Terminologie

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 la [RFC2119] et indiquent les niveaux d’exigence pour les mises en œuvre conformes.

2. Lignes directrices

Ces lignes directrices sont à l'usage des groupes de travail de l'IETF et des auteurs de protocoles qui déterminent si il faut rendre obligatoire la gestion automatique des clé ou si la gestion manuelle des clés est acceptable. Un jugement informé est nécessaire.

Le terme de "gestion de clés" se réfère à l'établissement de matériel de clés de chiffrement à utiliser avec un algorithme cryptographique pour fournir des services de sécurité de protocole, en particulier l'authentification, la protection de l'intégrité et de la confidentialité. La gestion de clé automatisée déduit une ou plusieurs clés de session à court terme. La fonction de déduction de clés peut faire usage de clés à long terme pour incorporer l'authentification dans le processus. La manière de distribuer cette clé à long terme aux homologues et le type de clé utilisée (valeur secrète symétrique pré partagée, clé publique RSA, clé publique DSA, et autres) sortent du domaine d'application du présent document. Cependant, cela fait partie de la solution globale de la gestion de clé. La gestion de clé manuelle est utilisée pour distribuer de telles valeurs. La gestion de clé manuelle peut aussi être utilisée pour distribuer des clés de session à long terme.

La gestion de clé automatique et la gestion de clé manuelle fournissent des caractéristiques très différentes. En particulier, le protocole associé à une technique de gestion de clé automatisée va confirmer la vivacité de l'homologue, protéger contre la répétition, authentifier la source de la clé de session à court terme, associer les informations d'état de protocole à la clé de session à court terme, et assurer qu'une clé de session de court terme fraîche est générée. De plus, un protocole de gestion de clé automatique peut améliorer l'interopérabilité en incluant un mécanisme de négociation des algorithmes cryptographiques. Ces caractéristiques précieuses sont impossibles ou extrêmement difficiles à réaliser avec la gestion de clé manuelle.

Pour certains algorithmes de chiffrement symétriques, les mises en œuvre doivent empêcher la sur utilisation d'une certaine clé. Une mise en œuvre de ces algorithmes peut faire usage de la gestion de clé automatisée lorsque les limites d'usage sont presque atteintes, afin de rétablir le remplacement des clés avant que les limites soient atteintes, maintenant ainsi la sécurité des communications.

Des exemples de système automatiques de gestion de clé incluent IPsec IKE et Kerberos. S/MIME et TLS incluent aussi des fonctions de gestion de clé automatique.

Les schémas de gestion de clé ne devraient pas être conçus par des amateurs ; il est presque certainement inapproprié que des groupes de travail conçoivent les leurs. Pour dire clairement les choses, le tout premier protocole de gestion de clé dans la littérature accessible a été publié en 1978 [NS]. Une faute et sa correction ont été publiées en 1981 [DS], et la correction a été cassée en 1994 [AN]. En 1995 [L], une nouvelle faute a été trouvée dans la version originale de 1978, dans un domaine non affecté par le problème de 1981/1994. Toutes ces fautes étaient évidentes une fois décrites – mais personne ne les avait vues auparavant. Noter que le protocole d'origine (traduit pour employer des certificats qui n'avaient pas été inventés à cette époque) faisait seulement trois messages.

Un logiciel de gestion de clés n'est pas toujours gros ou gonflé. Même IKEv1 [RFC2409] peut être fait en moins de 200 koctets de code objet, et TLS [RFC2246] en fait la moitié. Noter que cette estimation de TLS inclut aussi d'autres fonctionnalités.

Une clé de session est utilisée pour protéger une charge utile. La nature de la charge utile dépend de la couche où est appliqué le chiffrement symétrique.

En général, une gestion de clé automatisée DEVRAIT être utilisée pour établir des clé de session. Une forte justification est nécessaire dans la section des considérations sur la sécurité d'une proposition qui fait usage de la gestion de clé manuelle.

2.1 Gestion de clé automatisée

Une gestion de clé automatisée DOIT être utilisée si une des conditions suivante est satisfaite :
- Une partie doit gérer n^2 clés statiques, où n peut devenir grand.
- Un chiffrement de flux (comme RC4 [TK], AES-CTR [NIST], ou AES-CCM [RFC3610]) est utilisé.
- Une valeur d'initialisation (IV) peut être réutilisée, en particulier comme IV implicite. Noter que les IV explicites aléatoires ou pseudo aléatoires ne posent problème que si la probabilité de répétition est élevée.
- De grandes quantités de données peuvent devoir être chiffrées en peu de temps, causant de fréquents changements de la clé de session à court terme.
- Des clés de session à long terme sont utilisées par plus de deux parties. La diffusion groupée est une exception nécessaire, mais des normes de gestion des clés de diffusion groupée sont en cours d'élaboration afin d'éviter cela à l'avenir. Le partage de clés de session à long terme devrait généralement être déconseillé.

- L'environnement de fonctionnement probable est l'objet de fréquents changement du personnel (ou des appareils) ce qui cause de fréquents changements de la clé de session à court terme.

2.2 Gestion de clé manuelle

La gestion de clé manuelle peut être une approche raisonnable dans une des situations suivantes :
- L'environnement a une bande passante disponible très limitée ou un délai d'aller-retour très élevé. Les systèmes à clé publique tendent à exiger de longs messages et beaucoup de calculs ; des solutions de remplacement symétriques, comme Kerberos, exigent souvent plusieurs allers-retours et des interactions avec des tiers.
- L'information protégée a peu de valeur.
- Le volume total de trafic sur la durée de vie entière de la clé de session à long terme sera très faible.
- L'échelle de chaque déploiement est très limité.

Noter que les assertions sur de telles choses devraient souvent être examinée avec scepticisme. La charge de la démonstration que la gestion de clé manuelle est appropriée incombe à celui qui la propose – et cela place la barre très haut.

Les systèmes qui emploient la gestion de clé manuelle ont besoin de dispositions pour les changements de clés. Il DOIT y avoir un moyen pour indiquer quelle clé est utilisée pour éviter les problèmes durant les transitions. Les concepteurs DEVRAIENT esquisser les mécanismes plausibles pour déployer les nouvelles clés et remplacer les anciennes qui pourraient avoir été compromises. Si c'est bien fait, de tels mécanismes peuvent ultérieurement être utilisés par un schéma de gestion de clés additif.

Le manque de clarté sur les parties impliquées dans l'authentification n'est pas une raison valide pour éviter la gestion de clé. Cela tendrait plutôt à indiquer un problème plus profond du modèle de sécurité sous jacent.

2.3. Taille de clé et valeurs aléatoires

On trouvera des lignes directrices sur la taille des clé de chiffrement pour les clés publiques utilisées pour échanger des clés symétriques dans le BCP 86 [RFC3766].

Lorsque on utilise la gestion de clé manuelle, les valeurs secrètes partagées à long terme DEVRAIENT faire au moins 128 bits.

On trouvera les lignes directrices sur la génération de nombres aléatoires dans le BCP 106 [RFC4086].

Lorsque la gestion de clé manuelle est utilisée, les secrets partagés à long terme DOIVENT être des valeurs "aléatoires" imprévisibles, assurant qu'un adversaire n'aura pas de meilleur espoir que 50 % de chances de trouver la valeur après avoir cherché sur la moitié de l'espace de recherche.

3. Considérations sur la sécurité

Le présent document donne des lignes directrices aux groupes de travail et aux concepteurs de protocoles. La sécurité de l'Internet est améliorée lorsque une gestion de clé automatisée est employée.

L'inclusion de la gestion de clé automatisée ne signifie pas que soit interdite une interface pour la gestion de clé manuelle. En fait, la gestion de clé manuelle est très utile pour le débogage. Donc, les mises en œuvre devraient fournir une interface de gestion de clé manuelle pour cela, même si ce n'est pas spécifié par le protocole.

4. Références

Cette section contient les références normatives et les références pour information.

4.1 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)

[RFC3766] H. Orman, P. Hoffman, "Détermination de la force des clés publiques utilisées pour l'échange de clés symétriques", avril 2004. (BCP0086)

[RFC4086] D. Eastlake 3rd, J. Schiller, S. Crocker, "Exigences d'aléa pour la sécurité", juin 2005. (*Remplace* RFC1750) (BCP0106)

4.2 Références pour information

[AN] M. Abadi and R. Needham, "Prudent Engineering Practice for Cryptographic Protocols", Proc. IEEE Computer Society Symposium on Research in Security and Privacy, mai 1994.

[DS] D. Denning and G. Sacco. "Timestamps in key distributed protocols", Communication of the ACM, 24(8):533--535, 1981.

[L] G. Lowe. "An attack on the Needham-Schroeder public key authentication protocol", Information Processing Letters, 56(3):131--136, novembre 1995.

[NIST] National Institute of Standards and Technology. "Recommendation for Block Cipher Modes of Operation -- Methods and Techniques," NIST Special Publication SP 800-38A, décembre 2001.

[NS] R. Needham and M. Schroeder. "Using encryption for authentication in large networks of computers", Communications of the ACM, 21(12), décembre 1978.

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

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC3610] D. Whiting, R. Housley, N. Ferguson, "Compteur avec CBC-MAC (CCM)", septembre 2003. *(Information)*

[TK] Thayer, R. and K. Kaukonen. "A Stream Cipher Encryption Algorithm", Travail en cours.

Adresse des auteurs

Steven M. Bellovin
Department of Computer Science
Columbia University
1214 Amsterdam Avenue, M.C. 0401
New York, NY 10027-7003
téléphone : +1 212-939-7149
mél : bellovin@acm.org

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
téléphone : +1 703-435-1775
mél : housley@vigilsec.com

Déclaration complète de droits de reproduction

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.