Internet Engineering Task Force (IETF)
Request for Comments : 6649
BCP 179
RFC rendue obsolète : 1510
Catégorie : Bonnes pratiques actuelles
ISSN: 2070-1721

L. Hornquist Astrand, Apple, Inc.
T. Yu, MIT Kerberos Consortium
juillet 2012
RFC mises à jour : 1964, 4120, 4121, 4757
Traduction Claude Brière de L'Isle

Les algorithmes DES, RC4-HMAC-EXP, et autres algorithmes cryptographiques faibles sont déconseillés dans Kerberos

Résumé
Le protocole d'authentification de réseau Kerberos 5, spécifié à l'origine dans la RFC1510, peut utiliser la norme de chiffrement de données (DES, *Data Encryption Standard*) pour le chiffrement. Presque 30 ans après la première publication de DES, l'Institut National des normes et technologies (NIST) a finalement retiré la norme en 2005, reflétant un consensus établi depuis longtemps sur le fait que DES n'est pas suffisamment sûr. En 2008, des matériels du commerce coûtant moins de 15 000 $ US pouvaient casser les clés DES en moins d'une journée en moyenne. DES a fait son temps depuis longtemps. En conséquence, le présent document met à jour les RFC1964, RFC4120, RFC4121, et RFC4757 pour déconseiller l'utilisation de DES, RC4-HMAC-EXP, et autres algorithmes de chiffrement faibles dans Kerberos. Comme la RFC1510 (rendue obsolète par la RFC4120) ne prend en charge que DES, le présent document recommande la reclassification de la RFC1510 comme Historique.

1. Introduction

La spécification originale du protocole d'authentification de réseau Kerberos 5 [RFC1510] ne prend en charge que le chiffrement de la norme de chiffrement de données (DES, *Data Encryption Standard*). Depuis de nombreuses années, la communauté cryptographique a considéré que DES fournit une sécurité inadéquate, principalement à cause de sa petite taille de clé. En conséquences, le présent document recommande la reclassification de la [RFC1510] (rendue obsolète par la [RFC4120]) comme Historique et met à jour les spécifications qui se rapportent à Kerberos, [RFC1964], [RFC4120], et [RFC4121] pour déconseiller l'utilisation de DES et des autres algorithmes cryptographiques faibles dans Kerberos, y compris certaines sommes de contrôle et hachages sans clés, ainsi le type de chiffrement faible variante faible à 56 bits "export strength" de RC4 de la [RFC4757].

2. Notation des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DERAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la [RFC2119].

3. Spécifications affectées

La spécification originale de l'IETF pour Kerberos 5 [RFC1510] ne prend en charge que DES pour le chiffrement. La [RFC4120] rend obsolète la [RFC1510] et met à jour la spécification Kerberos pour inclure des algorithmes cryptographiques supplémentaires, mais permet encore l'utilisation de DES. La [RFC3961] décrit le système cryptographique Kerberos et inclut la prise en charge des types de chiffrement DES, mais elle ne spécifie pas de niveaux d'exigence pour aux.

La spécification du mécanisme d'interface de programmation d'application de service générique de sécurité Kerberos (GSS-API, *Generic Security Services Application Programming Interface*) de la [RFC1964] et sa version mise à jour [RFC4121] définit les mécanismes de somme de contrôle et de chiffrement sur la base de DES. Avec l'existence de nouveaux types de chiffrement pour la GSS-API Kerberos définie dans la [RFC4121], le mécanisme de GSS-API RC4 fondé sur HMAC de Microsoft, et le DES3 du MIT (qui n'est pas publié comme RFC) il n'est plus besoin de prendre en charge les vieux types d'intégrité (SGN) et de confidentialité (SEAL) fondés sur DES.

La [RFC4757] décrit les types de chiffrement RC4-HMAC utilisés par Microsoft Windows et permet une variante à 56 bits "export strength". (La constante de caractère "fortybits" utilisée dans sa définition est une référence historique et ne se réfère pas à la taille de clé réelle du type de chiffrement.)

4. Insécurité de DES

L'insécurité de DES est évidente depuis de nombreuses années. Même au moment de sa première publication, les cryptographes évoquaient la possibilité que 56 bits soit une trop petite taille de clé pour DES. L'Institut National des normes et technologies (NIST) a officiellement retiré DES en 2005 [DES-Withdrawal], et a aussi annoncé une période de transition qui s'est terminée le 19 mai 2007 [DES-Transition-Plan]. L'IETF a aussi publié sa position dans la [RFC4772], dans laquelle la recommandation résumée est très claire : "n'utilisez pas DES".

En 2006, des chercheurs on démontré la capacité à trouver une clé DES via une recherche en force brute dans une moyenne de moins de 9 jours en utilisant un matériel valant moins de 10 000 € [Break-DES]. En 2008, une compagnie offrait un matériel capable de casser une clé DES en moins d'un jour en moyenne [DES-1day] qui coûte moins de 15 000 $ [DES-Crack]. Les recherches en force brute de clé de DES sont de plus en plus rapides et moins chères. (La compagnie susmentionnée fait la promotion des son appareil pour la récupération en un click des clés DES perdues.) Il est clair qu'il est grand temps de retirer l'utilisation de DES de Kerberos.

5. Recommandations

Le présent document supprime les types RECOMMANDÉS suivants de la [RFC4120] :

Chiffrement : DES-CBC-MD5(3)

Sommes de contrôle : DES-MD5 (8, nommé RSA-MD5-DES dans la [RFC3961]).

Les mises en œuvre et déploiements de Kerberos NE DEVRAIENT PAS mettre en œuvre ou déployer les types de chiffrement de DES seul suivants : DES-CBC-CRC(1), DES-CBC-MD4(2), DES-CBC-MD5(3) (met à jour la [RFC4120]).

Les mises en œuvre et déploiements de Kerberos NE DEVRAIENT PAS mettre en œuvre ou déployer le type de chiffrement de variante RC4 "export strength" : RC4-HMAC-EXP(24) (met à jour la [RFC4757]). Le présent document n'ajoute aucune sorte d'exigence que les mises en œuvre conformes mettent en œuvre RC4-HMAC(23).

Les mises en œuvre et déploiements de Kerberos NE DEVRAIENT PAS mettre en œuvre ou déployer les types de somme de contrôle suivants : CRC32(1), RSA-MD4(2), RSA-MD4-DES(3), DES-MAC(4), DES-MAC-K(5), RSA-MD4-DES-K(6), RSA-MD5-DES(8) (met à jour la [RFC4120]).

Il est possible d'utiliser le type de somme de contrôle RSA-MD5(7) en toute sécurité, mais seulement avec une protection supplémentaire, telle que celle que fournit un authentifiant chiffré. Les mises en œuvre PEUVENT utiliser RSA-MD5 au sein d'un authentifiant chiffré pour la rétro compatibilité avec les systèmes qui ne prennent pas en charge des types plus récents de somme de contrôle (met à jour la [RFC4120]). Un exemple est que certains systèmes traditionnels prennent en charge RC4-HMAC(23) [RFC4757] pour le chiffrement lorsque DES n'est pas disponible ; ces systèmes utilisent les sommes de contrôle RSA-MD5 à l'intérieur d'authentifiants chiffrés avec RC4-HMAC.

Les mises en œuvre et déploiements de mécanisme GSS Kerberos NE DEVRAIENT PAS mettre en œuvre et déployer les ALG SGN suivantes : DES MAC MD5(0000), MD2.5(0100), DES MAC(0200) (met à jour la [RFC1964]).

Les mises en œuvre et déploiements de mécanisme GSS Kerberos NE DEVRAIENT PAS mettre en œuvre et déployer les ALG SEAL suivantes : DES(0000) (met à jour la [RFC1964]).

L'effet de ces deux dernières phrases est que le présent document déconseille le paragraphe 1.2 de la [RFC1964].

Le présent document recommande ici la reclassification de la [RFC1510] comme Historique.

6. Considérations pour la sécurité

Retirer le soutien à DES seul améliore la sécurité parce que DES est considéré comme non sûr. RC4-HMAC-EXP a une taille de clé similairement inadéquate, de sorte que supprimer sa prise en charge améliore aussi la sécurité.

Kerberos définit certains types de chiffrement qui sont soit sous spécifiés, soit n'avaient seulement que des allocations de numéro mais pas de spécifications. Les mises en œuvre devraient s'assurer qu'elle ne mettent en œuvre et activent que des types de chiffrement sûrs.

Les considérations pour la sécurité de la [RFC4757] continuent de s'appliquer à RC4-HMAC, incluant les faiblesses connues de RC4 et MD4, et le présent document ne change pas pour l'instant le statut d'Information de la [RFC4757]. La principale raison pour ne pas déconseiller activement l'utilisation de RC4-HMAC est que c'est le seul type de chiffrement qui interopère avec les plus anciennes versions de Microsoft Windows une fois que DES et RC4-HMAC-EXP sont retirés. Ces plus anciennes versions de Microsoft Windows seront vraisemblablement utilisées au moins jusqu'en 2015.

7. Remerciements

Mattias Amnefelt, Ran Atkinson, Henry Hotz, Jeffrey Hutzelman, Leif Johansson, Simon Josefsson, et Martin Rex ont relu ce document et fourni des suggestions pour des améliorations. Sam Hartman a proposé de passer la [RFC1510] au statut de Historique. Michiko Short a fourni des informations sur les dates de fin des versions de Windows.

8. Références

8.1 Références normatives

[RFC1964] J. Linn, "Mécanisme GSS-API de Kerberos version 5", juin 1996. (*MàJ par la* RFC6649)

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

[RFC3961] K. Raeburn, "Spécifications de chiffrement et de somme de contrôle pour Kerberos 5", février 2005.

[RFC4120] C. Neuman et autres, "Service Kerberos d'authentification de réseau (V5)", juillet 2005.

[RFC4121] L. Zhu et autres, "Version 2 du mécanisme d'interface de programme d'application de service de sécurité générique (GSS-API) de Kerberos version 5", juillet 2005. (*MàJ* RFC1964) *(P.S.)*

[RFC4757] K. Jaganathan et autres, "Types de chiffrement Kerberos RC4-HMAC utilisés par Windows de Microsoft", décembre 2006". *(Information)* (*MàJ par la* RFC6649)

8.2 Références pour information

[Break-DES] Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., Rupp, A., and M. Schimmler, "How to break DES for EUR 8,980", SHARCS'06 - Special-purpose Hardware for Attacking Cryptographic Systems, avril 2006, <http://www.copacobana.org/paper/copacobana_SHARCS2006.pdf>.

[DES-1day] SciEngines GmbH, "Break DES in less than a single day", <http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html>.

[DES-Crack] Scott, T., "DES Brute Force Cracking Efforts 1977 to 2010", 2010, <http://www.tjscott.net/security.extras/des.crack.efforts.pdf>.

[DES-Transition-Plan] National Institute of Standards and Technology, "DES Transition Plan", mai 2005, <http://csrc.nist.gov/groups/STM/common_documents/DESTranPlan.pdf>.

[DES-Withdrawal] National Institute of Standards and Technology, "Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation", Federal Register Vol. 70, No. 96, Document 05-9945, 70 FR 28907-28908, mai 2005, <http://www.gpo.gov/fdsys/pkg/FR-2005-05-19/pdf/05-9945.pdf>.

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

[RFC4772] S. Kelly, "Implications pour la sécurité de l'utilisation de la norme de chiffrement des données (DES)", décembre 2006. *(Information)*

Adresse des auteurs

Love Hornquist Astrand
Apple, Inc.
Cupertino, California
USA
mél : lha@apple.com

Tom Yu
MIT Kerberos Consortium
77 Massachusetts Ave.
Cambridge, Massachusetts
USA
mél : tlyu@mit.edu