Groupe de travail Réseau J. Schlyter, OpenSSH
Request for Comments : 4255 W. Griffin, SPARTA
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle janvier 2006

Utilisation du DNS pour la publication sécurisée d'empreintes digitales de clé Secure Shell (SSH)

Résumé
Le présent document décrit une méthode pour vérifier les clé d'hôtes Secure Shell (SSH) en utilisant la sécurité du système des noms de domaine (DNSSEC, *Domain Name System Security*). Le document définit un nouvel enregistrement de ressource du DNS qui contient une empreinte digitale de clé standard SSH.

Table des matières

1. Introduction

Le protocole SSH [RFC4251] fournit la connexion à distance sécurisée et d'autres services réseau sécurisés sur un réseau non sûr. La sécurité de la connexion s'appuie sur l'authentification du serveur lui-même auprès du client ainsi que sur l'authentification de l'utilisateur lui-même auprès du serveur.

Si une connexion est établie avec un serveur dont la clé publique n'est pas déjà connue du client, une empreinte digitale de la clé est présentée à l'utilisateur pour vérification. Si l'utilisateur décide que l'empreinte digitale est correcte et accepte la clé, la clé est sauvegardée localement et utilisée pour vérification pour toutes les connexions suivantes. Bien que certains utilisateurs soucieux de sécurité vérifient l'empreinte digitale hors bande avant d'accepter la clé, de nombreux utilisateurs acceptent aveuglément la clé présentée.

La méthode décrite ici peut assurer la vérification hors bande en cherchant l'empreinte digitale de la clé publique du serveur dans le DNS [RFC1034], [RFC1035] et en utilisant DNSSEC [RFC4033], [RFC4034], [RFC4035] pour vérifier la recherche.

Afin de distribuer l'empreinte digitale en utilisant le DNS, le présent document définit un nouvel enregistrement de ressource du DNS, "SSHFP", pour porter l'empreinte digitale.

La compréhension de base du système du DNS [RFC1034], [RFC1035] et des extensions de sécurité du DNS [RFC4033] [RFC4034] [RFC4035] est supposée par ce 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].

2. Vérification de clé d'hôte SSH

2.1 Méthode

À la connexion à un serveur SSH, le client SSH PEUT chercher le ou les enregistrements de ressource SSHFP pour l'hôte auquel il se connecte. Si l'algorithme et l'empreinte de la clé reçue du serveur SSH correspondent à l'algorithme et à l'empreinte d'un des enregistrements de ressource SSHFP retournés du DNS, le client PEUT accepter l'identité du serveur.

2.2. Notes de mise en œuvre

Les mises en œuvre de client DEVRAIENT fournir une politique configurable utilisée pour choisir l'ordre des méthodes utilisées pour vérifier une clé d'hôte. Le présent document définit une méthode : la mémorisation d'empreinte digitale dans le DNS. Une autre méthode définie dans l'architecture SSH [RFC4251] utilise des fichiers locaux pour mémoriser les clés aux fins de comparaison. D'autres méthodes qui pourraient être définies à l'avenir pourraient inclure de mémoriser les empreintes digitales dans LDAP ou d'autres bases de données. Une politique configurable va permettre aux administrateurs de déterminer quelles méthodes ils veulent utiliser et dans quel ordre de priorité. Cela va permettre aux administrateurs de déterminer quelle confiance ils veulent accorder aux différentes méthodes.

Un scénario spécifique pour avoir une politique configurable est celui où les clients n'utilisent pas les noms pleinement qualifiés d'hôte pour se connecter aux serveurs. Dans ce scénario, la mise en œuvre DEVRAIT vérifier la clé d'hôte dans une base de données locale avant de vérifier la clé via l'empreinte digitale retournée du DNS. Cela aiderait à empêcher un attaquant d'injecter un chemin de recherche DNS dans le résolveur local et de forcer le client à se connecter à un hôte différent.

2.3 Correspondance d'empreinte digitale

La clé publique et l'enregistrement de ressource SSHFP sont confrontés en comparant le numéro d'algorithme et l'empreinte digitale.

L'algorithme de clé publique et le numéro d'algorithme SSHFP DOIVENT correspondre.

Un résumé de message de la clé publique, utilisant l'algorithme de résumé de message spécifié dans le type d'empreinte digitale SSHFP, DOIT correspondre à l'empreinte digitale SSHFP.

2.4 Authentification

On NE DOIT PAS faire confiance à une clé publique vérifiée en utilisant cette méthode si l'enregistrement de ressource SSHFP utilisé pour la vérification n'a pas été authentifié par un enregistrement de ressource SIG de confiance.

Les clients qui valident eux-mêmes les signatures DNSSEC DEVRAIENT utiliser les procédures standard de validation DNSSEC.

Les clients qui ne valident pas eux-mêmes les signatures DNSSEC DOIVENT utiliser un transport sûr (par exemple, TSIG [RFC2845], SIG(0) [RFC2931], ou IPsec [RFC2411]) entre eux-mêmes et l'entité qui effectue la validation de signature.

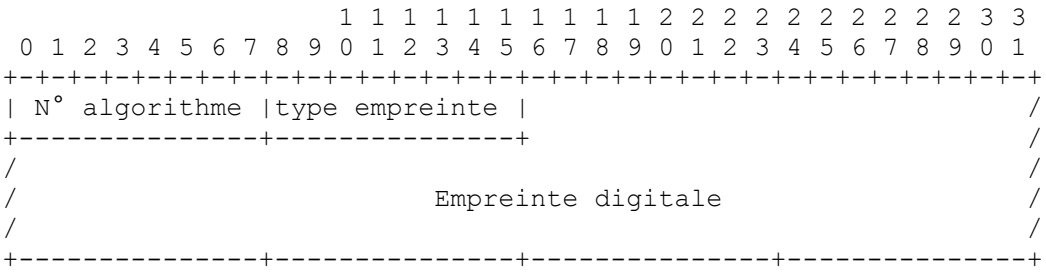
3. Enregistrement de ressource SSHFP

L'enregistrement de ressource (RR, *resource record*) SSHFP est utilisé pour mémoriser une empreinte digitale d'une clé publique d'hôte SSH qui est associée à un nom du système des noms de domaines (DNS, *Domain Name System*).

Le code du type de RR pour le RR SSHFP est 44.

3.1 Format de RDATA SSHFP

Le RDATA pour un RR SSHFP consiste en un numéro d'algorithme, un type d'empreinte digitale et en l'empreinte digitale de la clé publique d'hôte.



3.1.1 Spécification de numéro d'algorithme

Cet octet de numéro d'algorithme décrit l'algorithme de la clé publique. Les valeurs suivantes sont allouées :

Valeur	Nom d'algorithme
0	réservé
1	RSA
2	DSS

Réserver d'autres types exige le consensus de l'IETF [RFC2434].

3.1.2 Spécification du type d'empreinte digitale

L'octet de type d'empreinte digitale décrit l'algorithme de résumé de message utilisé pour calculer l'empreinte digitale de la clé publique. Les valeurs suivantes sont allouées :

Valeur	Type d'empreinte digitale
0	réservé
1	SHA-1

Réserver d'autres types exige le consensus de l'IETF [RFC2434].

Pou des raisons d'interopérabilité, aussi peu de types d'empreinte digitale que possible devraient être réservés. La seule raison de réserver des types supplémentaires est d'augmenter la sécurité.

3.1.3 Empreinte digitale

L'empreinte digitale est calculée sur la touffe de clé publique comme décrit dans la [RFC4253].

L'algorithme de résumé de message est présumé produire une chaîne opaque d'octets en résultat, qui est placée telle qu'elle dans le champ empreinte digitale des RDATA.

3.2 Format de présentation du RR SSHFP

Les RDATA du format de présentation de l'enregistrement de ressource SSHFP consistent en deux nombres (algorithme et type d'empreinte digitale) suivis par l'empreinte digitale elle-même, présentée en hexadécimal, par exemple :

host.exemple. SSHFP 2 1 123456789abcdef67890123456789abcdef67890

L'utilisation de mnémoniques à la place des nombres n'est pas permise.

4. Considérations sur la sécurité

Actuellement, le niveau de confiance qu'un utilisateur peut accorder de façon réaliste à une clé de serveur est proportionnel au niveau d'attention consacré à la vérification que la clé publique présentée correspond réellement à la clé privée du serveur. Si un utilisateur accepte une clé sans vérifier l'empreinte digitale avec quelque chose d'appris à travers un canal sécurisé, la connexion sera vulnérable à une attaque par interposition.

La sécurité globale de l'utilisation de SSHFP pour la vérification de la clé d'hôte SSH dépend des politiques de sécurité de l'administrateur de l'hôte SSH et de l'administrateur de la zone DNS (en transférant l'empreinte digitale), des aspects de détails de la façon dont la vérification est faite dans la mise en œuvre SSH, et de la diligence du client pour accéder au DNS d'une manière sûre.

Un de ces aspect est l'ordre dans lequel les empreintes digitales sont recherchées (par exemple, en vérifiant d'abord le fichier local et ensuite le SSHFP). On note que, en plus de protéger le transfert pour la première fois des clés d'hôtes, SSHFP peut facultativement être utilisé pour une plus forte protection de la clé d'hôte.

Si SSHFP est vérifié en premier, de nouvelles clés d'hôte SSH peuvent être distribuées en remplaçant la SSHFP correspondante dans le DNS.

Si la vérification de la clé d'hôte SSH peut être configurée à exiger la SSHFP, la révocation de clé d'hôte SSH peut être mise en œuvre en retirant la SSHFP correspondante du DNS.

Comme déclaré au paragraphe 2.2, on recommande que les mises en œuvre de SSH fournissent un mécanisme de politique pour contrôler les méthodes utilisées pour la vérification de la clé d'hôte. Un scénario spécifique pour avoir une politique configurable est lorsque les clients utilisent des noms d'hôte non qualifiés pour se connecter aux serveurs. Dans ce cas, on recommande que les mises en œuvre de SSH confrontent la clé d'hôte à une base de données locale avant de vérifier la clé via l'empreinte digitale retournée du DNS. Cela aidera à empêcher un attaquant d'injecter un chemin de recherche DNS dans le résolveur local et de forcer le client à se connecter à un hôte différent.

Une approche différente pour résoudre le problème de la recherche DNS serait que les clients utilisent un chemin de recherche DNS de confiance, c'est-à-dire, un chemin qui n'a pas été acquis par DHCP ou autres mécanismes d'autoconfiguration. Comme il n'y a aucun moyen avec les API de recherche de DNS actuelles de dire si un chemin de recherche vient d'une source de confiance, le système client entier va devoir être configuré avec ce chemin de recherche de DNS de confiance.

Un autre dépendance est celle de la mise en œuvre de DNSSEC elle-même. Comme déclaré au paragraphe 2.4, on rend obligatoire l'utilisation de méthodes sûres pour la recherche et que les RR SSHFP soient authentifiés par des RR SIG de confiance. Ceci est particulièrement important si la SSHFP doit être utilisée comme base du changement de clé d'hôte et/ou leur révocation, comme décrit ci-dessus.

Comme DNSSEC ne protège que l'intégrité de l'empreinte digitale de clé d'hôte après qu'elle est signée par l'administrateur de la zone DNS, l'empreinte digitale doit être transférée de façon sûre de l'administrateur d'hôte SSH à l'administrateur de la zone DNS. Cela pourrait être fait manuellement entre les administrateurs ou automatiquement en utilisant une mise à jour dynamique sûre du DNS [RFC3007] entre le serveur SSH et le serveur de noms. On note que ce n'est pas différent des autres situations de changement de clé, par exemple, un client qui envoie une demande de certificat à une autorité de certification pour qu'elle le signe.

5. Considérations relatives à l'IANA

L'IANA a alloué le code de type de RR 44 à SSHFP dans l'espace de type de RR standard.

L'IANA a ouvert un nouveau registre pour le type de RR SSHFP pour les algorithmes de clé publique. Les types définis sont :
0 est réservé
1 est RSA
2 est DSA

Ajouter de nouvelles réservations exige le consensus de l'IETF [RFC2434].

L'IANA a ouvert un nouveau registre pour le type de RR SSHFP pour les types d'empreinte digitale. Les types définis sont :
0 est réservé
1 est SHA-1

Ajouter de nouvelles réservations exige le consensus de l'IETF [RFC2434].

6. Références normatives

[RFC1034] P. Mockapetris, "Noms de domaines - Concepts et facilités", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936, 8020, 8482, 8767)

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767

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

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC4033] R. Arends, et autres, "Introduction et exigences pour la sécurité du DNS", mars 2005.

[RFC4034] R. Arends et autres, "Enregistrements de ressources pour les extensions de sécurité au DNS", mars 2005.

[RFC4035] R. Arends et autres, "Modifications du protocole pour les extensions de sécurité du DNS", mars 2005. *(P.S. ; MàJ par* RFC8198

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

[RFC4253] C. Lonvick, "Protocole de couche Transport Secure Shell (SSH)", janvier 2006. *(P.S., MàJ par* RFC6668, 8268, 8308, 8332, 8709)

7. Références pour information

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Obs., voir* RFC6071)

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645) *(P.S.)*

[RFC2931] D. Eastlake 3rd, "Signatures de demandes et de transactions du DNS (SIG(0))", septembre 2000. *(P.S.)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000.

8. Remerciements

Les auteurs remercient de leurs contributions Martin Fredriksson, Olafur Gudmundsson, Edward Lewis, et Bill Sommerfeld

Adresse des auteurs

Jakob Schlyter
OpenSSH
812 23rd Avenue SE
Calgary, Alberta T2G 1N8
Canada
mél : jakob@openssh.com
URI : http://www.openssh.com/

Wesley Griffin
SPARTA
7075 Samuel Morse Drive
Columbia, MD 21046
USA
mél : wgriffin@sparta.com
URI : http://www.sparta.com/

Notice de marque commerciale

"ssh" est une marque commerciale déposée au États Unis d'Amérique et/ou dans d'autres pays.

Déclaration complète de droits de reproduction

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