rfc6024

Exigences de gestion d'ancre de confiance

Une ancre de confiance représente une entité autoritative via une clé publique et des données associées. La clé publique est utilisée pour vérifier les signatures numériques, et les données associées sont utilisée pour contraindre les types d'informations pour lesquelles l'ancre de confiance a autorité. Un tiers de confiance utilise les ancres de confiance pour déterminer si un objet signé numériquement est valide en vérifiant une signature numérique en utilisant la clé publique de l'ancre de confiance, et en forçant les contraintes exprimées dans les données associées pour l'ancre de confiance. Ce document décris certains problèmes associées avec le manque de mécanisme de gestion d'ancre de confiance et définis les exigences pour les formats de données et les protocoles conçus pour adresser ces problèmes.

Les signatures numériques sont utilisées dans de nombreuses applications. Pour que les signatures numériques fournissent l'intégrité et d'authentification, la clé publique utilisée pour vérifier la signature numérique doit être "trustée", par exemple, accepté par un tiers de confiance comme utilisation appropriée dans le contexte donné. Une clé publique utilisée pour vérifier une signature doit être configurée comme une ancre de confiance ou contenue dans un certificat qui peut être vérifiée par une chemin de certification se terminant à l'ancre de confiance. Une ancre de confiance est une clé publique et ses données associées utilisée par un tiers de confiance pour valider une signature sur un objet signé où l'objet est soit :

- Un certificat à clé publique qui commence un chemin de certification terminé par un certificat de signature ou un certificat de chiffrement.
- Un objet, autre qu'un certificat à clé publique ou liste de révocation de certificat, qui ne peut pas être validé via l'utilisation d'un chemin de certification.

Les ancres de confiance ont seulement une signification locale, par exemple, chaque tiers de confiance (RP) est configuré avec un jeu d'ancres de confiance, soit par le RP ou par l'entité qui gère les TA dans le contexte dans lequel le RP opère. Les données associées définissent le périmètre d'une ancre de confiance en imposant des contraintes sur les signatures qui peuvent être vérifiés en utilisant l'ancre de confiance. Par exemple, si une ancre de confiance est utilisée pour vérifier les signatures dans le certificats X.509, ces contrainte peuvent inclure une combinaison d'espace de noms, de stratégie de certificat, ou de types d'application/utilisation.

Une utilisation des signatures numérique est la vérification des signatures dans les packages de firmware chargés dans les modules hardware, tels que les modules cryptographiques, boitiers de cables, routeurs, etc. Vu que de tels périphériques sont souvent gérés à distance, les périphériques doivent être capable d'authentifier la source d'interaction de gestion et peuvent utiliser les ancres de confiance pour effectuer cette interaction. Cependant, les ancres de confiance nécessitent également une gestion. D'autres applications nécessitant une gestion d'ancre de confiance incluent les navigateurs web (qui utilisent les ancres de confiance en authentifiant les serveurs web) et les clients mail (qui utilisent les ancres de confiance en validant les email signés et en authentifiant les bénéficiaires des mails chiffrés).

Toutes les applications qui valident les signatures numériques valide les moyens de gérer un ou plusieurs jeux d'ancre de confiance. Chaque jeu d'ancre de confiance est référé dans ce document à un magasin d'ancres de confiance. Souvent, la manière de gérer les magasins d'ancre de confiance est spécifique à l'application et compte sur des moyens tiers pour établir et maintenir la fiabilité. Une application peut utiliser plusieurs magasins d'ancre de confiance, et un magasin d'ancre de confiance peut être utilisé par plusieurs applications. Chaque magasin d'ancre de confiance est gérée par au moins un gestionnaire TA ; un gestionnaire TA peut gérer plusieurs magasins TA.

Les exigences statuées dans ce document ont été préparés avant la publication des rfc5914 et rfc5934. Le document n'a pas été publié à ce moment pour permettre des changement dans les exigences durant le développement des spécification technique associées. Les exigences décrites ci-dessous sont celles qui ont été considérées durant le développement des rfrc5914 et rfc5934.

Cette section fournis une introduction et définis la terminologie de base. La section suivante décris les problèmes avec les méthodes de gestion d'ancre de confiance actuelles. Les sections suivantes décrivent les exigences et considérations de sécurité pour une solution de gestion d'ancre de confiance.

Terminologie

Les termes suivants sont définis pour pouvoir fournir un vocabulaire pour les exigences décrites pour la gestion des ancres de confiance.

Trust Anchor Une ancre de confiance représente une entité autoritative via une clé publique et ses données associées. La clé publique est utilisée pour vérifier les signatures numériques, et les données associées sont utilisées pour contraindre les types d'information pour lesquels l'ancre de confiance est autoritative. Un tiers de confiance utilise les ancres de confiance pour déterminer si un objet signé numériquement est valide en vérifiant une signature numérique utilisant la clé publique de l'ancre de confiance, et en forçant les contraintes exprimées dans les données associées pour l'ancre de confiance.

Trust Anchor Manager Un gestionnaire d'ancre de confiance est une entité responsable de la gestion du contenu d'un magasin d'ancre de confiance. Tout au long de ce document, chaque gestionnaire d'ancre de confiance est assumé être représenté comme, ou délégué par une ancre de confiance distincte.

Trust Anchor Store Un magasin d'ancre de confiance est un jeu d'une ou plusieurs ancres de confiance stockés dans un périphérique. Un magasin d'ancre de confiance peut être géré par un ou plusieurs gestionnaire d'ancre de confiance. Un périphérique peut avoir plus d'un magasin d'ancre de confiance, chaque pouvant être utilisé par une ou plusieurs applications.

Énoncé des problèmes

Les ancres de confiance sont utilisées pour supporter de nombreux scénarios d'application. Beaucoup de navigateurs internet et le clients mail utilisent les ancres de confiance lors de l'authentification de sessions TLS, en vérifiant les mails signés, et en générant des mails chiffrés en validant un chemin de certification avec le certificat du serveur, le certificat de l'émetteur d'un mail, ou le certificat du destinataire d'un mail. De nombreuses distributions de logiciels sont signées numériquement pour permettre l'authentification des sources du logiciel avant l'installation. Les ancres de confiance qui supportent ces application sont typiquement installés comme partie de l'OS ou application, installés durant un système de gestion de configuration de l'entreprise, ou installé directement par un OU ou une utilisateur.

Les ancres de confiance sont généralement stockés dans des magasins d'ancre de confiance spécifique à l'application ou spécifique à l'OS. Souvent, une simple machine peut avoir de nombreux magasins d'ancre de confiance qui ne peuvent pas être synchronisés. Examiner le contenu d'un magasin d'ancre de confiance particulier implique généralement l'utilisation d'un outil propriétaire qui interagi avec un type particulier de magasin.

La présence d'une ancre de confiance dans un magasin particulier véhicule souvent l'autorisation implicite de valider les signatures pour tous les contextes pour lequel le magasin est accédé. Par exemple, la clé publique d'une autorité d'horodatage peut être installée dans un magasin pour valider les signatures dans les horodatages. Cependant, si le magasin contenant ce TA est utilisé par plusieurs applications qui servent différents bit, la même clé pourrait être utilisée de manière inappropriée pour valider d'autres types d'objets tels que les certificats ou les réponses OCSP. Avant la publication de la rfc5914, il n'y avait pas de mécanisme standard pour limiter le périmètre d'une ancre de confiance. Une pratique commune pour adresser ce problème est de placer différents TA dans différents magasins et de limiter le jeu d'application qui accèdent à un magasin TA donné.

La relation de confiance entre les PKI sont négociées par des autorité de stratégie. Les négociations exigent fréquemment un temps significatif pour s'assurer que toutes exigences des parties participantes sont satisfaites. Ces exigences sont exprimées, dans une certaine mesure, dans les certificats à clé publique via les contraintes de stratégie, les contraintes de noms, etc. Pour pouvoir forcer ces exigences, les magasins d'ancre de confiance doivent être gérés en accord avec les intensions d'autorité de stratégie. Sinon, les contraintes définies dans un cross-certificat pourrait être contournées en reconnaissant le sujet du cross-certificat comme ancre de confiance, qui permettrait d'implémenter des traitement de chemin qui évitent le cross-certificat.

Les ancres de confiance sont souvent représentés comme des certificats autos-signés, qui ne fournissent généralement aucun moyen d'établir la validité de l'information contenu dans le certificat. La confiance dans l'intégrité d'une ancre de confiance est généralement établie via un moyen externe, souvent en vérifiant l'empreinte du certificat auto-signé avec une source autoritative. Les Opérations de routine d'ancre de confiance nécessitent généralement de telles vérifications externe, si la livraison de la clé d'une ancre de confiance est supportée par CMP. Idéalement, seul le jeu initial d'ancres de confiance qui sont installés dans un magasin de confiance particulier nécessitent une vérification tiers proportionnée avec les exigences de sécurité des applications en utilisant le magasin.

Malgré d'utilisation répandue des ancres de confiance, il n'y a ni standard pour la découverte du jeu d'ancres de confiance installés dans un magasin particulier ni de moyen standard de gérer ces ancres de confiance. Le reste de ce document décris les exigences pour une solution à ce problème avec certaines considérations de sécurité.

Exigences

Cette section décris les exigences pour un protocole de gestion d'ancre de confiance. Les exigences sont fournies pour le contenu d'une ancre aussi bien que les opération de gestion des magasins.

Indépendance de transport

Une solution générale pour la gestion des ancres de confiance doit être indépendant du transport pour pouvoir s'appliquer à divers environnements de communication. Il doit fonctionner dans des environnements orientés session et store-and-forward aussi bien que dans les modèles push and pull. Pour répondre à tous ces modèles de manière uniforme, l'intégrité sans connexion et l'authentification de l'origine des données pour les transaction TA doivent être fournis au niveau applicatif. La confidentialité peut être fournie pour de telles transactions.

Raisonnement

Tous les périphériques qui utilisent les ancres de confiance ne sont pas disponible pour des opérations de gestion online ; certains périphériques peut nécessiter une interaction manuelle pour la gestion des ancres de confiance. L'authentification de l'origine des données et l'intégrité sont requis pour s'assurer que la transaction n'a pas été modifiée en route. Seul l'intégrité sans connexion est requise, pour compatibilité avec les contextes store-and-forward.

pré-requis fonctionnels

Au minimum, un protocole utilisé pour la gestion d'ancre de confiance doit permettre à un gestionnaire d'ancre de confiance d'effectuer les opérations suivantes :

- Déterminer quels ancres de confiance sont installées dans un magasin particulier
- Ajouter une ou plusieurs ancres de confiance à un magasin
- Supprimer une ou plusieurs ancres de confiance d'un magasin
- Remplacer tout un magasin

Un protocole le gestion d'ancre de confiance doit fournir un support pour ces opérations basiques ; cependant, toutes les implémentations ne supportent pas chaque options. Par exemple, certaines implémentations peuvent supporter seulement le remplacement des magasins.

Ces exigences décrivent les opérations requises pour gérer le contenu d'un magasin d'ancre de confiance. Une opération d'édition a été omise pour des raisons de simplicité, avec des suppressions consécutives et opérations d'ajouts utilisés dans ce but. Une simple opération d'ajout ou suppression peut agir sur plus d'une ancre de confiance pour éviter les aller-retours inutiles et sont fournis pour éviter le besoins de toujours remplacer tout un magasin. Le remplacement d'un magasin peut être utile comme une opération alternative aux opérations d'ajouts et suppression.

Gestion des cibles

Une protocole pour la gestion TA doit permettre à une transaction TA d'être dirigée vers :

- Tous les magasins TA dont le manager est responsable
- Une liste énumérée d'un ou plusieurs groupes nommés de magasins

- un magasin d'ancre de confiance individuel

Les connexions entre les PKI peuvent être accomplies en utilisant différents moyens. La cross-certification unilatérale ou bilatérale peut être effectuée, ou une communauté peut simplement élire pour accepter explicitement une ancre de confiance depuis une autre communauté. Généralement, ces décisions se font dans l'entreprise. Dans certains scénarios, il peut être utile d'établir ces connexions pour une petite communauté dans une entreprise. Les mécanismes des grandes entreprises, tel que les cross-certificats sont mal adaptés à cet effet vu que la révocation du certificat affecte l'ensemble de l'entreprise.

Un protocole de gestion d'ancre de confiance peut adresser ce problème en supportant l'installation limitée des ancres de confiance (ex, l'installation des TA dans des sous-jeux de communauté d'utilisateurs de l'entreprise), et en supportant l'expression des contraintes dans l'utilisation des ancres de confiance par des tiers de confiance. L'installation limitée nécessite la capacité d'identifier les membre de la communauté qui sont destinés à s'appuyer sur une ancre de confiance particulière, et la capacité de vérifier et reporter le contenu des magasins. Les contraintes d'ancre de confiance peuvent être utilisés pour représenter les limitations qui peuvent être exprimées dans un cross-certificat, et l'installation limitée assure que la reconnaissance de l'ancre de confiance ne comprend par nécessairement toute une entreprise.

Les configuration d'ancre de confiance peuvent être uniforme dans une entreprise, ou peuvent être unique à une simple application ou un petit jeu d'applications. De nombreux périphériques et certaines application utilisent plusieurs magasins. En fournissant un moyen d'adresser un magasin spécifique ou une collection de magasins, un protocole de gestion d'ancre de confiance peut permettre une gestion efficace de tous les magasins sous le contrôle d'un gestionnaire d'ancre de confiance.

Délégation de l'autorité du gestionnaire TA

Un protocole de gestion d'ancre de confiance doit permettre un transfert sécurité du contrôle d'un magasin d'ancre de confiance d'une manager à un autre. Il devrait également permettre la délégation pour les opérations spécifiques sans nécessiter de délégation de toutes les capacités de gestion d'ancres de confiance.

Le renouvellement de clé du gestionnaire d'ancre de confiance est un type de transfert qui doit être supporté. Dans ce cas, la nouvelle clé sera assignée aux mèmes privilèges que l'ancienne clé.

La création des ancres de confiance pour des buts spécifiques, tels que la signature de firmware, est un autre exemple de délégation. Par exemple, un gestionnaire d'ancre de confiance peut déléguer seulement d'autorité de signer des firmware à une entité, mais interdit d'autres délégations de ce privilège, ou le gestionnaire d'ancre de confiance peut autorisé la délégation à d'autres autorités de signature de firmwares délégués à d'autres entités.

Support rfc 5280

Un protocole de gestion d'ancre de confiance doit permettre la gestion des ancres de confiance qui seront utilisé pour valider les chemins de certification et les CRL en accord avec les rfc5280 et rfc5055. Un format d'ancre de confiance doit permettre la représentation de contraintes qui influencent la validation de chemin de certification ou l'établissement de périmètre d'utilisation de la clé publique de l'ancre de confiance. Des exemples de telles contraintes sont les contraintes de noms, les stratégies de certificat, et l'utilisation de clé.

La validation de chemin de certification est une des applications d'ancre de confiance les plus communes. Les règles pour utiliser les ancres de confiance pour la validation de chemin sont établis dans la rfc5280. La rfc5055 décris l'utilisation des ancres de confiance pour la validation de chemin déléguée. Les ancres de confiance utilisée pour valider les chemins de certification sont responsable de la livraison, possiblement via une délégation, des informations de statut de révocation des certificats qu'il émet ; c'est souvent accomplis en signant une CRL.

Autres supports

Un protocole de gestion d'ancre de confiance doit permettre la gestion des ancres de confiance qui peuvent être utilisé pour d'autres buts que la validation de chemin de certification, incluant les ancres de confiance qui ne peuvent pas être utilisé pour la validation de chemin de certification. Il devrait être possible d'autoriser une ancre de confiance à déléguer l'autorité (à d'autres TA ou propriétaires de certificat) et d'empêcher une ancre de confiance d'être délégué.

Les ancres de confiance sont utilisées pour valider une variété d'objets signés, pas seulement les certificats à clé publique et les CRL. Par exemple, une ancre de confiance peut être utilisée pour vérifier les packages de firmware (rfc5108), les réponses OCSP (rfrc2560), les réponses SCVP (rfc5055), ou les horodatages (rfc3161). Les TA qui sont autorisées pour l'utilisation de certains de ces types d'opérations ne peuvent pas être autorisés pour vérifier les certificats à clé publique ou les CRL. Donc, il est important d'être capable d'imposer des contraintes sur la manière dont un TA donné est employé.

Format d'ancre de confiance

Au minimum, un protocole de gestion d'ancre de confiance doit supporter la gestion des ancres de confiances représentés comme certificats auto-signés et les ancres de confiance représentés comme un nom distinct, informations de clé publique, et, optionnellement, les données associées. La définition d'une ancre de confiance doit inclure une clé publique, un algorithme de clé publique, et, si nécessaire, les paramètres de la clé publique. Quand la clé publique est utilisée pour valider les chemins de certification ou les CRL, un nom distinct doit également être inclus (rfc5280). Un format d'ancre de confiance doit permettre la spécification d'un identifiant de clé publique pour permettre à d'autres applications d'ancre de confiance, par exemple, la vérification des données signées en utilisant la structure SignedData (CMS - rfc5652). Un format d'ancre de confiance devrait également permettre la représentation des contraintes qui peuvent être appliquées pour restreindre l'utilisation d'une ancre de confiance.

Avant la publication de la rfc5914, il n'y avait pas de format d'ancres de confiance. Les certificats X.509 auto-signés sont généralement utilisés, mais la rfc5280 ne mandate par la représentation d'ancre de confiance particulier. Elle exige seulement que les information de clé publique de l'ancre de confiance et le nom distinct soit disponible durant la validation du chemin de certification. CMS est largement utilisé pour protéger divers types de contenu en utilisant les signatures numériques, incluant le contenu qui peut être vérifié directement en utilisant une ancre de confiance, tels que les packages de firmware. Les contraintes peuvent inclure une périodes de validité, des contraintes sur la validation de chemin de certification, etc.

Authentification

Une entité reçevant une donnée de gestion d'ancre de confiance doit être capable d'authentifier l'identité du partie en fournissant les informations et doit être capable de confirmer que le partie est autorisé à fournir ces informations.

Un gestionnaire d'ancre de confiance doit être capable d'authentifier quel magasin d'ancre correspond à un listing du contenu du magasin et être capable de confirmer que le contenu du listing n'a pas été altéré.

L'authentification de l'origine des données et l'intégrité sont requis pour supporter les opération de gestion à distance, même quand les transaction de gestion des TA sont effectuées via des communications store-and-forward.

Réduire la dépendance des mécanimes tiers

En effectuant des opérations d'ajout, un protocole de gestion d'ancre de confiance devrait permettre de vérifier automatiquement l'intégrité des TA par un tiers de confiance sans s'appuyer sur des mécanismes tiers.

Traditionnellement, une ancre de confiance est distribuée via un mécanisme tiers avec vérification manuelle de l'intégrité avant l'installation. L'installation est généralement effectuée par quelqu'un avec suffisamment de privilèges administratifs dans le système recevant l'ancre de confiance. La fiabilité des mécanismes de confiance tiers est un problème avec les approches de gestion des ancre de confiance actuelles, et la réduction du besoin de mécanismes tiers est une motivation principale pour le développement de mécanismes de

gestion d'ancre de confiance. Idéalement, les mécanismes tiers sont requis seulement durant l'initialisation du magasin.

Détection des répétitions

Un protocole de gestion d'ancre de confiance doit permettre aux participants engagés dans l'échange du protocole de gestion de détecter les attaques replay. Un mécanisme de détection de replay qui n'introduit pas d'exigence pour une source sûre de temps doit être disponible. Les mécanismes qui ne nécessitent pas de source sûre de temps peuvent être disponibles.

La détection de replay des transactions de gestion d'ancre de confiance est requise pour supporter les opérations de gestion distantes. Le replay d'anciennes transaction pourraient résulter en la réintroduction d'ancres de confiance compromises. Certains périphériques qui utilisent les ancres de confiance n'ont pas accès à une source de temps sûre, donc un mécanisme de détection de replay qui nécessite une source de temps sûre est insuffisant.

Compromission ou récupération après sinistre

Un protocole de gestion d'ancre de confiance doit permettre la récupération lors de la compromission ou la perte de la clé privée d'une ancre de confiance, incluant la clé privée autorisée à service de gestion d'ancre de confiance, sans nécessiter la ré-initialisation du magasin.

La compromission ou la perte d'une clé privée correspondant à une ancre de confiance peut avoir des conséquences négatives significatives. Actuellement, dans certains cas, la ré-initialisation de tous les magasin affectés est requise pour récupérer lors d'une perte ou d'une compromission d'une clé d'ancre de confiance. À cause du coût associés avec la ré-initialisation, un protocole de gestion d'ancre de confiance devrait supporter les options de récupération qui ne nécessitent pas de ré-initialisation du magasin.

Considérations de sécurité

La clé publique utilisé pour authentifier une transaction de gestion TA peut avoir été placée dans le client comme résultat d'une première transaction de gestion TA ou durant une configuration initiale. Dans de nombreux scénarios, au moins une clé publique autorisé pour la gestion d'ancre de confiance doit être placée dans chaque magasin d'ancre de confiance. Cette clé publique peut être transporté et vérifiée en utilisant des moyens tiers. Dans tous les scénarios, sans regarder le mécanisme d'authentification, au moins un gestionnaire d'ancre de confiance doit être établis pour chaque magasin d'ancre de confiance durant la configuration initiale du magasin.

La compromission d'une clé privée d'une ancre de confiance peut résulter en de nombreux problèmes de sécurité, incluant l'émission de sécurité compromis ou des ancres de confiance volé.

L'utilisation de contraintes basées sur l'ancre de confiance nécessite une grande attention en définissant les ancres de confiance. Des erreurs de la part d'un gestionnaire pourrait résulter des déni de service ou des conséquences de sécurité sérieuses. Par exemple, si une contrainte de nom pour une ancre de confiance qui sert de racine d'une PKI inclus une faute de frappe, il en résulte un déni de service pour les propriétaires de certificats. Si un gestionnaire d'ancre de confiance délègue par inadvertance tous ses privilège et les délégations suppriment le gestionnaire d'ancre de confiance des magasins d'ancre de confiance sous son contrôle, la récupération peut nécessiter la ré-initialisation de tous les magasins d'ancre de confiance affectés.

La rfc5280 nécessite que la validation de chemin de certificat soit initialisée avec un nom du sujet TA et une clé publique, mais n'exige pas le traitement d'autres information, tels quel les contraintes de nom. L'inclusion de contraintes dans les ancres de confiance est optionnelle. Quand des contraintes sont explicitement incluse par un gestionnaire d'ancre de confiance en utilisant un protocole de gestion d'ancre de confiance, on s'attend à ce que l'algorithme de validation de chemin de certification utilise ces contraintes. Les propriétaires d'application doivent confirmer l'implémentation de traitement de chemin supportant le traitement des contraintes basées sur TA, si requis.

De nombreuses considération de sécurité de la rfc5280 sont également applicable à la gestion des ancres de confiance.