Chapitre 5: Gestion de clefs de chiffrement

Polytech Nancy

Année 2021/2022

Bases cryptographiques (rappel)

Chiffrement symétrique :

- pour chiffrer $\{M\}_K$,
- et déchiffrer $\{\{M\}_K\}_K = M$.

Chiffrement asymétrique :

- clef publique pour chiffrer $\{M\}_{PK_A}$,
- clef privée pour déchiffrer $\{\{M\}_{PK_A}\}_{SK_A} = M$ ou signer $\{M\}_{SK_A}$

Fonctions de hachage :

- non inversibles ; exemple : $M, \{h(M)\}_{SK_A}$

Nonce :

- nombre aléatoire créé par un utilisateur.

Gestion de clefs

Point route

Gestion des clefs

Principales opérations

- Génération
- Transfert
- Vérification
- Stockage

Génération des clefs

Espaces de clefs réduits

- Codage restreint, caractères choisis, clefs faibles, ...

Mauvais choix de clefs

- Lettres mnémotechniques, ... $\rightarrow$ attaque par dictionnaire

Clefs aléatoires

- Générateurs, broyage de clef, acronyme, ...

Phrases mots de passe

- Broyage de clef

Transfert de clef

- Physiquement
  - Rencontre, canal de transmission protégé, ... $\rightarrow$ rarement possible
- Un tiers choisit et fournit la clef
- Employer une clef précédente pour chiffrer une nouvelle clef
- Si A et B ont des communications sûres avec un tiers C, C peut relayer la clef entre A et B

Vérification de clefs

- Origine
  - Rencontre physique
  - Annuaire
  - Tiers
- Moyens
  - Fonction de hachage
  - Certificat

Stockage des clefs

- Fichiers
- Support extérieur
  - *Bande magnétique*
  - Token, carte ROM, clef USB
  - Carte à puce
- Ajout de code supplémentaire
  - PIN
  - Sur-chiffrement

Remarques

- Utilisation d'un centre de distribution de clefs (KDC).
- Nécessité d'avoir des hiérarchies de KDC pour de grands réseaux, mais ils doivent se faire confiance.
- La durée de vie des clefs de session devrait être limitée pour une plus grande sécurité.
- Contrôle de buts d'utilisation des clefs.

Point route

Clefs symétriques

- Nécessité pour les deux usagers de partager une clef secrète commune.
- Comment distribuer sûrement cette clef ?
- L'échec d'un système sûr est souvent dû à une rupture dans le schéma de distribution des clefs.

Scénario de distribution de clefs symétriques

1. $A \rightarrow KDC : \ Request, N_1$
2. $KDC \rightarrow A : \ \{K_s, Request, N_1\}_{K_a}, \{K_s, ID_a\}_{K_b}$
3. $A \rightarrow B : \ \{K_s, ID_a\}_{K_b}$
4. $B \rightarrow A \ : \{N_2\}_{K_s}$
5. $A \rightarrow B : \ \{f(N_2)\}_{K_s}$

- Étapes de distribution de la clef : 1-3
- Étapes d'authentification : 3-5

Clefs publiques

- Le chiffrement par clef publique permet de résoudre les problèmes de distribution de clefs.
- On peut employer soit
  - Annonce publique
  - Annonce publiquement disponible
  - Autorité de clef publique
  - Certificat de clef publique

Annonce publique

- Distribution des clefs publiques directement aux destinataires ou par broadcast à la communauté dans son ensemble.
  - *Exemple :* apposer les clefs de PGP aux méls ou les poster dans des forums ou mailing-lists.
- Risque : la contrefaçon
  - N'importe qui peut créer une clef en prétendant être quelqu'un d'autre et la publier.
  - La mascarade peut continuer tant que la contrefaçon n'est pas découverte.

Annuaire public

- Enregistrement des clefs dans un annuaire public.
- Nécessité de faire confiance à cet annuaire.
- Propriétés :
  - Doit contenir les entrées (nom, clef publique).
  - Possibilité de s'inscrire de manière sécurisée dans l'annuaire.
  - Possibilité de remplacer la clef à tout moment.
  - Publié périodiquement.
  - Possibilité de consultation électronique.

Autorité de clef publique

- Renforcement du contrôle de la distribution des clefs à partir de l'annuaire.
- Dispose des mêmes propriétés qu'un annuaire.
- Chaque participant doit disposer d'une paire de clefs.
  - Publication de la clef publique dans l'annuaire.
- Interaction avec l'autorité pour obtenir la clef publique du correspondant.
  - Exige l'accès en temps réel à l'annuaire quand les clefs sont nécessaires.

Scénario de distribution de clefs publiques

1. $A \rightarrow PKA : \ Request, Time_1$
2. $PKA \rightarrow A : \ \{PK_b, Request, Time_1\}_{SK_{auth}}$
3. $A \rightarrow B : \ \{ID_a, N_1\}_{PK_b}$
4. $B \rightarrow PKA : \ Request, Time_2$
5. $PKA \rightarrow B : \ \{PK_a, Request, Time_2\}_{SK_{auth}}$
6. $B \rightarrow A \ : \{N_1, N_2\}_{PK_a}$
7. $A \rightarrow B : \ \{N_2\}_{PK_b}$

Certificat de clefs publiques

- Les certificats permettent l'échange de clef sans accès en temps réel à l'autorité de clef publique.
- Un certificat lie une identité à une clef publique.
  - Habituellement avec d'autres informations telles que la période de validité, les droits d'utilisation, ...
- Son contenu est signé par la clef privée d'une entité de confiance (ou autorité de certification, CA).
- Il peut être vérifié par toute personne connaissant la clef publique de l'autorité de certification.

Scénario d'échange de certificats de clefs publiques

1. $A \rightarrow CA : \ PK_a$
2. $CA \rightarrow A : \ C_A = \{Time_1, ID_a, PK_a\}_{SK_{auth}}$

---

1. $B \rightarrow CA : \ PK_b$
2. $CA \rightarrow B : \ C_B = \{Time_2, ID_b, PK_b\}_{SK_{auth}}$

---

1. $A \rightarrow B : \ C_A$
2. $B \rightarrow A \ : C_B$

Clefs de session

- Distribution de clef publique : simple ; permet la confidentialité et/ou l'authentification ; mais lent !
- Objectif : protection du contenu d'un message
- Solution : système hybride + clef de session
- Souhait : disposer de plusieurs solutions alternatives pour négocier une session

Distribution simple de clef de session

Merkle, 1979

- A produit une nouvelle paire de clefs publique/privée provisoire.
- A envoie à B sa clef publique et son identité.
- B engendre une clef de session K_s et l'envoie à A, chiffrée par la clef publique fournie par A.
- A déchiffre la clef de session et tous les deux peuvent l'utiliser.

Scénario de distribution simple de clef de session

1. $A \rightarrow B : \ PK_a, ID_a$
2. $B \rightarrow A : \ \{K_s\}_{PK_a}$

Scénario de distribution simple de clef de session

1. $A \rightarrow B : \ PK_a, ID_a$
2. $B \rightarrow A : \ \{K_s\}_{PK_a}$

Problème : attaque « man in the middle ».

Scénario de distribution simple de clef de session

1. $A \rightarrow B : \ PK_a, ID_a$
2. $B \rightarrow A : \ \{K_s\}_{PK_a}$

Problème : attaque « man in the middle ».

1. $A \rightarrow I(B) : \ PK_a, ID_a$
1′. $I(A) \rightarrow B : \ PK_i, ID_a$
2′. $B \rightarrow I(A) : \ \{K_s\}_{PK_i}$
2. $I(B) \rightarrow A : \ \{K_s\}_{PK_a}$
3. $A \rightarrow I(B) : \ \{M\}_{K_s}$

Scénario de distribution de clef de session avec confidentialité et authentification

1. $A \rightarrow B : \{N_1, ID_a\}_{PK_b}$
2. $B \rightarrow A : \{N_1, N_2\}_{PK_a}$
3. $A \rightarrow B : \{N_2\}_{PK_b}$
4. $A \rightarrow B : \{\{K_s\}_{SK_a}\}_{PK_b}$

Point route

Exemple de protocole d'authentification

Needham-Schroeder, 1978

- But : établissement d'une clef de session symétrique K_{AB} pour A et B, qui doit être fraîche.
- Utilisation d'une tierce partie de confiance T.

Construction pas à pas...

Exemple de protocole d'authentification

Solution 1

1. $A \rightarrow T : \ A, B$
2. $T \rightarrow A : \ K_{ab}$
3. $A \rightarrow B : \ K_{ab}, A$

Correct ?

Exemple de protocole d'authentification

Solution 2

1. $A \rightarrow T : \ A, B$
2. $T \rightarrow A : \ \{K_{ab}\}_{K_{at}}, \{K_{ab}\}_{K_{bt}}$
3. $A \rightarrow B : \ \{K_{ab}\}_{K_{bt}}, A$

Correct ?

Exemple de protocole d'authentification

Solution 3

1. $A \rightarrow T : \ A, B$
2. $T \rightarrow A : \ \{K_{ab}, B\}_{K_{at}}, \{K_{ab}, A\}_{K_{bt}}$
3. $A \rightarrow B : \ \{K_{ab}, A\}_{K_{bt}}$

Correct ?

Exemple de protocole d'authentification

Solution 4

1. $A \rightarrow T : \ A, B, N_a$
2. $T \rightarrow A : \ \{K_{ab}, B, N_a, \{K_{ab}, A\}_{K_{bt}}\}_{K_{at}}$
3. $A \rightarrow B : \ \{K_{ab}, A\}_{K_{bt}}$
4. $B \rightarrow A : \ \{N_b\}_{K_{ab}}$
5. $A \rightarrow B : \ \{N_b - 1\}_{K_{ab}}$

Correct ?

Exemple de protocole d'authentification

Solution 5

1. $B \rightarrow A : \ B, N_b$
2. $A \rightarrow T : \ A, B, N_a, N_b$
3. $T \rightarrow A : \ \{K_{ab}, B, N_a\}_{K_{at}}, \{K_{ab}, A, N_b\}_{K_{bt}}$
4. $A \rightarrow B : \ \{K_{ab}, A, N_b\}_{K_{bt}}$

Correct ?

Exemple de protocole d'authentification

Variante sous Kerberos

1. $A \rightarrow T : \ A, B, N_a$
2. $T \rightarrow A : \ \{K_{ab}, B, N_a, \{K_{ab}, A\}_{K_{bt}}\}_{K_{at}}$
3. $A \rightarrow B : \ \{N_a\}_{K_{ab}}, \{K_{ab}, A\}_{K_{bt}}$
4. $B \rightarrow A : \ \{N_a - 1, N_b\}_{K_{ab}}$
5. $A \rightarrow B : \ \{N_b - 1\}_{K_{ab}}$

Exemple de protocole d'échange de clef

Diffie-Hellman, 1976

- Méthode d'échange de clef secrète ou de session.
- Utilisé dans de nombreux produits commerciaux (SSL).
- Permet d'établir une clef commune connue seulement des deux participants.
- La valeur de la clef dépend des participants.
- Basée sur l'élévation à la puissance dans un champ fini (facile).
- La sécurité se fonde sur la difficulté de calculer des logarithmes discrets (difficile).

Exemple de protocole d'échange de clef

Principe de l'algorithme de Diffie-Hellman

- Soient A et B les deux parties de la communication.
- A engendre un nombre premier p et un primitif a (tous deux sont publics).
- A et B engendrent chacun un nombre aléatoire, x_A et x_B.
- Ils s'échangent a élevé à la puissance de leur nombre aléatoire, modulo p.
- Ils calculent alors la clef commune $a^{x_A x_B}$.

Point route

Point route

Certificat électronique

Problématique (exemple)

- Un utilisateur connaît la clef publique d'une personne en consultant, par exemple, un serveur Web ou un serveur LDAP.
- Mais comment garantir que la clef publique de A que B a récupérée est correcte ?
- Cette clef pourrait avoir été déposée par une autre personne, ou les données sur le serveur pourraient avoir été piratées.

Certificat électronique

Définition

- C'est comme une carte d'identité ou un passeport.
- Il contient des informations concernant son propriétaire, sa signature, une date de validité, une présentation spécifique,. . . permettant de reconnaître ce document comme non contrefait, et délivré par une autorité connue.
- C'est un document électronique, résultat d'un traitement fixant les relations existant entre une clef, son propriétaire et l'application pour laquelle il a été émis.
  - Pour une personne, il prouve l'identité de celle-ci.
  - Pour une application, il assure que celle-ci n'a pas été détournée de ses fonctions.
  - Pour un site, il offre la garantie lors d'un accès que l'on est sur le bon site.

Certificat électronique

Informations contenues :

- numéro de série du certificat ;
- désignation de l'autorité émettrice du certificat ;
- période de validité ;
- nom distinctif du titulaire de la clef ;
- identification de l'algorithme de chiffrement et valeur de la clef ;
- informations complémentaires optionnelles (mél,. . .) ;
- identification de l'algorithme de signature et valeur de la signature.

La signature électronique est calculée à partir de ces informations, chiffrée par la clef privée de l'autorité de certification délivrant ce certificat.

Certificats électroniques

Classes de certificats

- Classe 1 : pas de contrôle d'identité du détenteur du certificat.
- Classe 2 : contrôle sur pièces, la preuve de l'identité est nécessaire.
- Classe 3 : présentation physique du demandeur requise.
- Classe 3+ : classe 3 avec en plus un support physique (carte à puce, clef USB,...)

Point route

Infrastructure de gestion de clefs

Problématique

- Lors d'une demande de certificat, décider...
  - ...qui va recueillir et vérifier les informations données ?
  - ...suivant quelles procédures ?
  - ...qui va créer le certificat ?
  - ...qui va le délivrer ?
  - ...pour quelle durée ?
  - ...où le stocker ?
  - ...où récupérer les certificats d'autres personnes ?
  - ...comment supprimer un certificat ? (expiration, compromission)
- Définir une *architecture de gestion des certificats* (IGC ou PKI, *Public Key Infrastructure*).

PKI : constituants

Objets

- Bi-clefs (clef privée / clef publique), certificats

Éléments

- Autorité de certification
- Autorité d'enregistrement
- Système de publication/distribution de certificats (annuaire)
- Applications compatibles avec la PKI

PKI : bi-clefs

Couple de clefs permettant la mise en œuvre d'algorithmes de chiffrement asymétrique.

Quatre types de bi-clefs

- Bi-clefs de confidentialité : pour chiffrer de petits messages.
- Bi-clefs de signature : pour signer des messages et vérifier les signatures.
- Bi-clefs de certification : pour signer les certificats ou des messages de révocation.
- Bi-clefs d'échange/transport de clefs : pour transporter des clefs symétriques utilisées pour sécuriser des communications.

PKI : Autorité d'enregistrement

Rôle

- Vérifie l'identité du demandeur de certificat.
- S'assure qu'il possède un coupe de clefs privée/publique.
- Récupère la clef publique.
- Transmet ces informations à l'autorité de certification.

Remarque : communication sécurisée entre l'AE et l'AC (authentification, intégrité, confidentialité).

PKI : Autorité de certification

- Délivre des certificats électroniques.
- A son propre certificat (auto-signé ou signé par une autre AC).
- Utilise sa clef privée pour signer les certificats délivrés.
- Se porte garante de l'identité du propriétaire d'un certificat qu'elle a délivré.
- A besoin d'être « reconnue ».

PKI : Autorité de certification

Rôle

- Reçoit les demandes de création de certificats des AE.
- Vérifie la validité de la signature des messages reçus.
- S'assure de l'intégrité de la demande et de l'authentification des émetteurs.
- Crée et signe les certificats avec sa clefs privée.
- Envoie les certificats aux utilisateurs et aussi au service de publication.

PKI : Autorité de certification commerciale

Quelques exemples (entreprises)

- BNP Paribas (Net Identity)
- CertEurope (CertEurope Classe 3+)
- CertiNomis (SociePoste),
- Crédit Agricole (CA Certificat)
- LCL (CL Authentis)

Trois types de certificats

- certificats serveurs
- certificats utilisateurs
- certificats Java

PKI : Service de publication

Rôle

- Rend disponibles les certificats émis par l'AC.
- Publie la liste des certificats valides.
- Publie la liste des certificats révoqués.

Possible par un annuaire LDAP ou un serveur Web.

PKI : révocation d'un certificat

Nombreuses raisons

- Fin de validité.
- Départ de l'entreprise.
- Changement de service.
- Perte de la clef privée.

PKI : révocation d'un certificat

- Chaque AC publie régulièrement la liste des certificats révoqués (CRL), signée par l'AC.
- Vérification d'un certificat :
  - vérification de la signature de l'AC l'ayant délivré ;
  - consultation de la CRL.

Problème : publication non instantanée.
Solution : interrogation d'un service de révocation (mais pb de sécurité de la communication).

Point route

Utilisations des certificats

Application et protocoles

- Courrier électronique sécurisé (S-MIME).
- Protocoles SSL/TLS : Web sécurisé (HTTPS), accès à la messagerie (IMAPS/SMTP).
- Réseaux virtuels privés (IPsec).
- En remplacement d'une authentification par mot de passe de l'utilisateur.

Utilisations des certificats

S/MIME

Secure Multipurpose Internet Mail Extensions

- Permet la signature et/ou le chiffrement des messages électroniques.
- Supporté par les principaux outils de messagerie, qui créent et vérifient les signatures.

Utilisations des certificats

SSL/TLS

Secure Socket Layer / Transport Layer Security

- SSL : protocole initialement développé par Netscape ; à partir de la version 3, standardisé par l'IETF.
- Dans une application client-serveur, grâce aux certificats, permet d'authentifier les extrémités et d'assurer la confidentialité et l'intégrité des échanges de données.
- S'insère entre l'application (*http*) et la couche transport (*tcp*).
- Quand la session est établie entre le client et le serveur, toutes les données transitant sont chiffrées et authentifiées.

Utilisations des certificats

SSH

Secure Shell

- Ensemble d'outils permettant d'avoir des sessions interactives en mode telnet ou X, des transferts de fichiers, des exécutions de commandes à distance.
- Authentification forte de l'utilisateur et du serveur ; chiffrement des données transmises.
- Utilise des algorithmes de chiffrement asymétriques avec une clef de session : bi-clefs engendré par l'utilisateur ; clef publique transmise au serveur.
- *Remarque :* n'utilise pas de certificats, mais à combiner avec.

Utilisations des certificats

IPsec

IP security

- Permet de chiffrer les paquets circulant sur un réseau, et d'authentifier les deux éléments physiques qui dialoguent.
- Certificats appartenant aux équipements (routeur ou station).
- N'authentifie pas les utilisateurs ou les serveurs.

Point route

Exemple : Service d'authentification X.509

Qu'est-ce ?

- Créé en 1988 dans le cadre de la norme X.500.
- Définit le cadre pour des services d'authentification (formats standards de certificats électroniques, algorithme pour la validation de chemins de certification).
- Repose sur un système hiérarchique d'autorités de certification.
- Souvent utilisé dans les protocoles d'authentification.
- Utilise la cryptographie à clef publique et les signatures digitales (RSA recommandé mais non imposé).

Certificat X.509

Version
Numéro de série
Algorithme de signature du certificat
Nom du signataire du certificat
Validité (dates limites)
Détenteur du certificat
Informations sur sa clef publique (algo, clef)
Identifiant unique du signataire
Identifiant unique du détenteur
Extensions
Signature des informations ci-dessus

Exemple : Pretty Good Privacy (PGP)

Qu'est-ce ?

- Programme gratuit de protection du mél, par Ph. Zimmermann.
- Utilise
  - IDEA pour le chiffrement,
  - RSA pour la gestion des clefs et les signatures digitales,
  - MD5 comme fonction de hachage à sens unique.
- Messages chiffrés ayant une structure de sécurité en couches (et non hiérarchique).

PGP : originalité

Gestion des clefs distribuée

- Pas d'autorité de certification : remplacée par un « climat de confiance ».
- Chaque utilisateur engendre et distribue sa propre clef publique.
- Les utilisateurs signent mutuellement leurs clefs publiques, et sont libres de décider à qui ils font confiance.

Exemple

A et B sont amis, tout comme B et C.
Si A veut communiquer avec C, il utilise un certificat émis par B.

Point route

Gestion des certificats en cours

Opérations

- Révocation
- Mise à jour
- Renouvellement

Exemples

- Mise à jour de la clef de l'AC.
- Renouvellement d'un certificat d'utilisateur.

Mise à jour de la clef de l'AC

Principales causes

- Certificat de l'AC arrivé à expiration.
- Clef privée compromise.

Autres causes

- Modification de la taille des clefs pour renforcer la sécurité.
- ...

Mise à jour de la clef de l'AC

Processus de modification de la clef publique

- Création d'un nouveau bi-clefs.
- Création d'un nouveau certificat contenant l'ancienne clef publique signée avec la nouvelle (*ancien-avec-nouveau*).
- Création d'un nouveau certificat contenant la nouvelle clef publique signée avec l'ancienne (*nouveau-avec-ancien*).
- Création d'un nouveau certificat contenant la nouvelle clef publique signée avec la nouvelle clef privée (*nouveau-avec-nouveau*).
- Publication des nouveaux certificats.

Mise à jour de la clef de l'AC

Dès lors, les certificats issus de l'AC sont signés avec la nouvelle clef privée.

Démarches

Pour un utilisateur possédant l'ancienne clef publique et voulant vérifier un certificat signé avec le nouvelle clef privée...

- récupérer le certificat *nouveau-avec-ancien*, pour obtenir la nouvelle clef publique.

Pour un utilisateur possédant la nouvelle clef publique et voulant vérifier un certificat signé avec l'ancienne clef privée...

- récupérer le certificat *ancien-avec-nouveau*, pour obtenir l'ancienne clef publique.

Mise à jour de la clef de l'AC

Durées de validité

- Certificat *ancien-avec-nouveau* : débute à la création de l'ancienne clef publique ; termine à sa date d'expiration.
- Certificat *nouveau-avec-ancien* : débute à la génération de la nouvelle clef publique ; termine à la date d'expiration de l'ancienne clef publique.
- Certificat *nouveau-avec-nouveau* : débute à la génération de la nouvelle clef publique ; termine à la date de la prochaine mise à jour du couple de clef.

Renouvellement d'un certificat d'utilisateur

Comme pour un contrat de travail...

- renouvellement (possible) en conservant les mêmes informations,
- sauf le numéro de série (unique),
- et les dates de validité (*pas avant*, *pas après*).

Renouvellement en fin de validité, mais aussi avant ou après.

- Renouvellement par demande à son AC.
- L'AC lui délivre le nouveau certificat.

Renouvellement d'un certificat d'utilisateur

Exemple : carte bancaire

- Carte émise pour une personne, pour une durée limitée.
- Carte renouvelée automatique ou après demande du client.
- Une fois renouvelée, l'ancienne carte est inutilisable (car expirée ou révoquée).

Point route

PKI : conclusion

Certificats numériques

- Partie intégrante de notre vie quotidienne (cartes bancaires, certificats logiciels, ...).
- Nombreux usages validés par l'IETF.
- Usage prédéfini à la création.

PKI : gestion des certificats

- Opérations : révocation, mise à jour, renouvellement.
- Problème de confiance : quel degré de confiance aux autorités de certification ?
- Révocation suite à compromission de clef privée : approches et performances variées.

Crédits

- Laurence Herbiet, Univ. Liège
- Maryline Maknavicius, Univ. Evry
- Équipe Pesto, LORIA