Chapitre : Protocoles cryptographiques

Définition

Protocole : Une séquence d'étapes de communication et de calcul.

Protocole cryptographique : C'est un protocole qui se base sur la cryptographie pour assurer certains objectifs de sécurité.

Notations

Messages :

Identité d'un principal : A, B, C, etc.

Identité d'un serveur : S.

Nonces : Na, Nb, etc.

Message m encrypté avec une clé k : $\{m\}_k$.

Message composé : m, m'.

Étapes de communication :

i: A –> B : m

Notations (suite)

- Exemple :

$$\begin{array}{llll} 1 & A & \longrightarrow B & : \quad N_a \\ 2 & B & \longrightarrow A & : \quad \{N_a\}_{k_b^{-1}} \end{array}$$

- Rôle vs. principal :
  - Principal : c'est un agent qui participe dans une session de l'exécution du protocole.
  - Rôle : c'est une abstraction du protocole où l'emphase est mise sur un seul agent.

Notations (suite)

- Nonce, timestamp : permettent d'assurer la fraîcheur d'un message.
  - Sans fraîcheur :

$$1 \quad A \longrightarrow B : \text{ es-tu là}$$
$$2 \quad B \longrightarrow A : \{\text{ oui, je suis là}\}_{k_b^{-1}}$$

  - Avec fraîcheur :

$$1 \quad A \longrightarrow B : \text{ es-tu là}, N_a$$
$$2 \quad B \longrightarrow A : \{\text{ oui, je suis là}, N_a\}_{k_b^{-1}}$$

$$1 \quad A \longrightarrow B : \text{ es-tu là}$$
$$2 \quad B \longrightarrow A : \{\text{ oui, je suis là}, T_b\}_{k_b^{-1}}$$

➪ Classification : Les protocoles cryptographiques peuvent être classés selon plusieurs critères.

- ➜ Systèmes cryptographiques : un protocole peut se baser sur une cryptographie symétrique, cryptographie asymétrique ou cryptographie symétrique et asymétrique à la fois.
- ➜ Objectif du protocole : authentification, distribution de clés, etc.
- ➜ Nombre d'étapes : 1 passe, 2 passes, etc.
- ➜ Utilisation ou non d'un serveur.
- ➜ Etc.

Protocoles d'authentification

- Authentification de l'identité : Permettre à un principal de prouver son identité à un autre.
  - Sécurité : Ne pas permettre à un principal X de prouver que son identité est Y $(X \neq Y)$.
- Authentification de messages (intégrité) : S'assurer que le contenu d'un message n'a pas été modifié.
  - Sécurité : Si un message est malicieusement ou accidentellement modifié en cours de route alors le récepteur devrait être capable de détecter cette modification.

Protocoles d'authentification

- Approches d'authentification :
  - Quelque chose que tu as : Signature manuelle, empreintes digitales, ADN, etc.
  - Quelque chose que tu possèdes : Clé physique, sceau, carte d'accès, etc.
  - Quelque chose que tu connais : NIP, mot de passe, clé secrète, etc.

Protocoles d'authentification

➪ Protocole de Woo et Lam (Exemple I) :

- ➜ C'est une authentification unidirectionnelle. Seul le principal A qui a besoin de prouver son identité au principal B.
- ➜ On passe par un serveur.
- ➜ Il se base sur des clés symétriques.

$$
\begin{array}{llcll}
1 & A & \longrightarrow & B & : \quad A \\
2 & B & \longrightarrow & A & : \quad N_b \\
3 & A & \longrightarrow & B & : \quad \{N_b\}_{k_{as}} \\
4 & B & \longrightarrow & S & : \quad \{A, \{N_b\}_{k_{as}}\}_{k_{bs}} \\
5 & S & \longrightarrow & B & : \quad \{N_b\}_{k_{bs}}
\end{array}
$$

Protocoles d'authentification

- Protocole de Woo et Lam (Exemple II) :
  - C'est une authentification bidirectionnelle. Le principal A a besoin de prouver son identité au principal B et vice-versa.
  - On passe par un serveur.
  - Il se base sur des clés symétriques.

$$
\begin{array}{lll}
1 & A \longrightarrow B : & A, N_a \\
2 & B \longrightarrow A : & B, N_b \\
3 & A \longrightarrow B : & \{A, B, N_a, N_b\}_{k_{as}} \\
4 & B \longrightarrow S : & \{A, B, N_a, N_b\}_{k_{as}} \{A, B, N_a, N_b\}_{k_{bs}} \\
5 & S \longrightarrow B : & \{B, N_a, N_b\}_{k_{as}} \{A, N_a, N_b\}_{k_{bs}} \\
6 & B \longrightarrow A : & \{B, N_a, N_b\}_{k_{as}}
\end{array}
$$

Protocoles d'authentification

- Protocole de Needham et Shroeder (Exemple III) :
  - C'est une authentification bidirectionnelle.
  - Il se base sur des clés asymétriques.

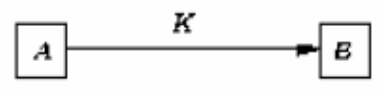
$$
\begin{array}{lll}
1 & A \longrightarrow B : & \{N_a, A\}_{k_b} \\
2 & B \longrightarrow A : & \{N_a, N_b\}_{k_a} \\
3 & A \longrightarrow B : & \{N_b\}_{k_b}
\end{array}
$$

Protocoles de distribution de clés

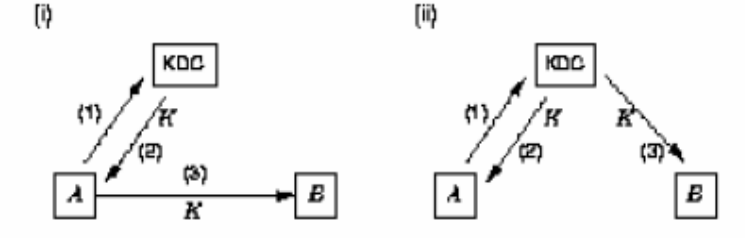
- Objectif : distribuer de nouvelles clés aux principaux pour qu'ils s'en servent pendant leurs communications futures.
- Sécurité :
  - Confidentialité : Non divulgation de la clé à un principal qui n'est pas supposé la connaître.
  - Intégrité : Toute modification de la clé devrait être détectée par ses récepteurs.

Protocoles de distribution de clés

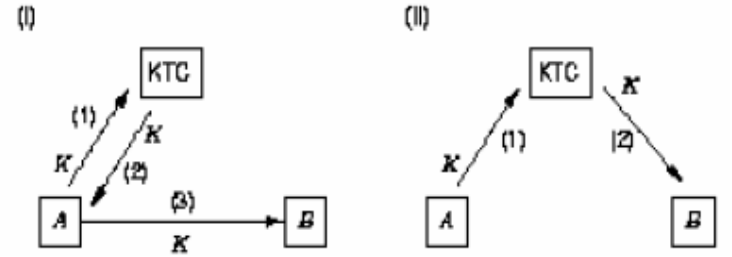
- Distribution des clés symétriques : Plusieurs scénarios possibles de distribution de clés.
  - Clé générée par A et envoyée à B :



  - Clé générée par un KDC (Key Distribution Center) et envoyée à A et B :



  - Clé générée par A, approuvée par un KTC (Key Translation Center) et envoyée à B :



Protocoles de distribution de clés

➪ Protocole de Carlson (Exemple I) :

- ➜ Un protocole à clés symétriques qui distribue des clés symétriques.
- ➜ Dans ce protocole S est un KDC.

$$
\begin{array}{lll}
1 & A \longrightarrow B : & A, N_a \\
2 & B \longrightarrow S : & A, N_a, B, N_b \\
3 & S \longrightarrow B : & \{k_{ab}, N_b, A\}_{k_{bs}}, \{N_a, B, k_{ab}\}_{k_{as}} \\
4 & B \longrightarrow A : & \{N_a, B, k_{ab}\}_{k_{as}}, \{N_a\}_{k_{ab}}, N'_b \\
5 & A \longrightarrow B : & \{N'_b\}_{k_{ab}}
\end{array}
$$

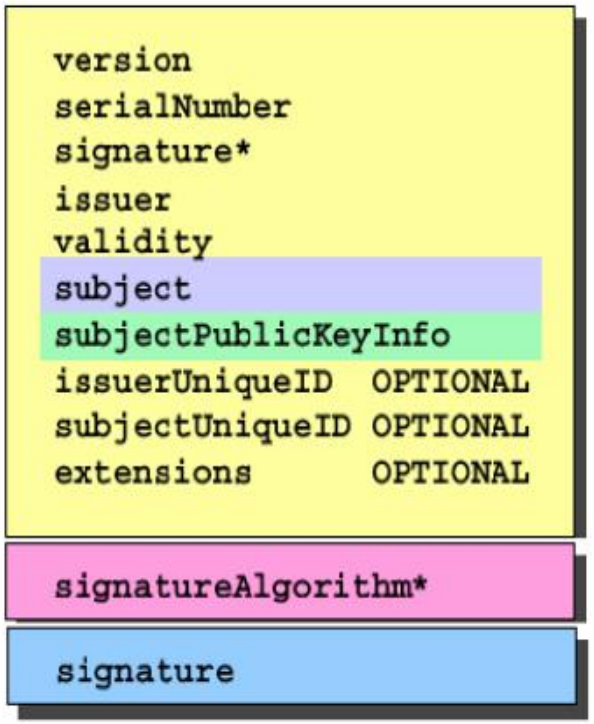
Protocoles de distribution de clés

- Distribution des clés publiques : Comment peut-on s'assurer qu'une clé publique est bien celle d'un principal donné ?
  - Nous avons besoin d'un moyen sûr qui nous permette de lier la clé publique à son vrai détenteur.
  - Plusieurs solutions :
    - Prendre la clé directement de la vraie personne (main à main).
    - Utiliser un mécanisme de certification.
    - Etc.

Protocoles de distribution de clés

➪ Distribution des clés publiques (suite) :

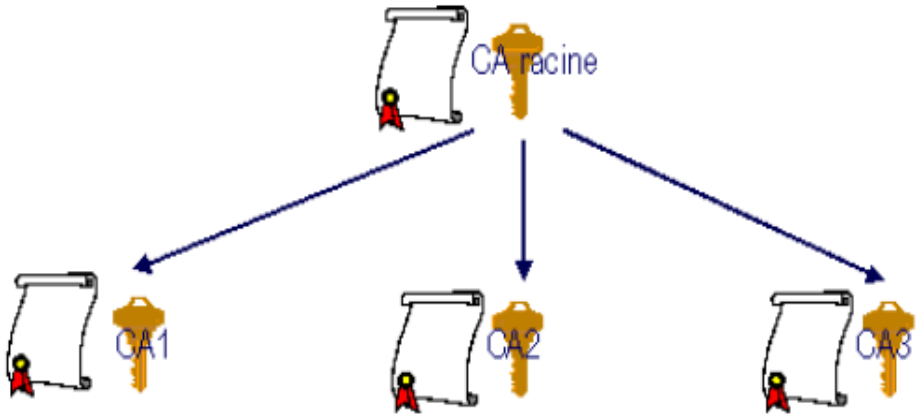
➜ Certificat : Un message signé permettant de lier une identité avec une clé publique.



➜ Autorité de certification (CA) : Un organisme de confiance qui sera chargé d'émettre des certificats.

Protocoles de distribution de clés

- Distribution des clés publiques (suite) :
  - Qui signe le certificat d'une CA ?
  - Plusieurs solutions :
    - La CA peut signer son propre certificat (auto-certification).
    - La CA fait signer son certificat par une autre CA, (la confiance est déplacée vers un autre CA).



  - Pour vérifier un certificat, on a parfois besoin d'obtenir la chaîne complète de certificats jusqu'à la racine.

Protocoles de distribution de clés

➪ Distribution des clés publiques (suite) :

➜ Protocole de Needham et Shroeder :

$$
\begin{array}{lll}
1 & A \longrightarrow S : & A, B \\
2 & S \longrightarrow A : & \{k_b, B\}_{k_s^{-1}} \\
3 & A \longrightarrow B : & \{N_a, A\}_{k_b} \\
4 & B \longrightarrow S : & B, A \\
5 & S \longrightarrow B : & \{k_a, A\}_{k_s^{-1}} \\
6 & B \longrightarrow A : & \{N_a, N_b\}_{k_a} \\
7 & A \longrightarrow B : & \{N_b\}_{k_b}
\end{array}
$$

➜ Remarque : Dans ce protocole S joue le rôle d'un CA.