TELECOM ParisTech - Université Pierre et Marie Curie
Master Réseaux (M2), Examen SECRES

Février 2015, *Durée 2h*

Documents non autorisés (à l'exception des corrigés des TD)

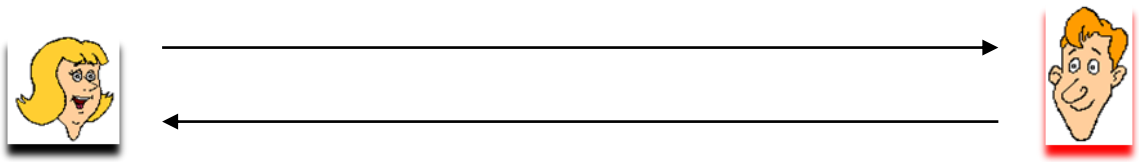
Partie 1 : Exercices (12 points)

Exercice 1 : Services de sécurité

On suppose qu'Alice veut envoyer un message *M* à Bob. Pour ce faire, Alice et Bob peuvent potentiellement utiliser un certain nombre de méthodes cryptographiques, qui sont décrites dans le tableau suivant :

M	Message en clair (*plaintext*)
A || B	Concaténation de A et B
K_A K^{-1}_A	Clé publique d'Alice Clé privée d'Alice
K_B K^{-1}_B	Clé publique de Bob Clé privée de Bob
E_k	Chiffrement asymétrique RSA en utilisant la clé publique K
s_k	Clé de chiffrement symétrique
AES_{sk}	Chiffrement à clé symétrique en utilisant AES-256 avec la clé s_k
$HMAC_{sk}$	*Keyed-Hash Message Authentication Code*
SHA	Fonction de hachage SHA-256
Sign	Signature numérique

On suppose que les clés publiques ont été distribuées en toute sécurité. Alice et Bob désirent avoir, dans leur communication, les propriétés suivantes : la confidentialité, l'intégrité, l'authentification et la non-répudiation. Pour chacun des cas ci-dessous, expliquer quelles sont les propriétés de sécurité qui sont protégées en prenant en considération la présence d'Eve (attaque de MITM).



Alice Bob

a) Alice envoie à Bob : E_{KA} (M || Sign K^{-1}_A (SHA(M)))

Le message est confidentiel, mais personne n'est capable de le déchiffrer même le destinataire. Alice est la seule qui est capable de le déchiffrer …..

b) Alice envoie à Bob : E_{KB} (M), Sign K^{-1}_A (SHA(M))

Confidentialité, non-répudiation, intégrité et authentification.

c) Alice génère une clé symétrique s_k et envoie à Bob : $E_{KB}(s_k)$, $E_{K^{-1}A}$ (SHA(s_k)), AES_{sk}(M)

Confidentialité de la clé + non-répudiation + authenticité, confidentialité du message

d) Alice génère deux clés symétriques s_{k1} et s_{k2} et envoie à Bob :

$E_{KB}(s_{k1})$, $E_{KB}(s_{k2})$, AES_{sk1} (M), $HMAC_{sk2}$ (SHA(M)), $Sign_{K^{-1}_A}$ (SHA(sk1)), $Sign_{K^{-1}_A}$ (SHA(sk2))

Les 4 services de sécurité

Exercice 2 : Attaques DDoS

L'entreprise TopSecurity vend un nouveau logiciel pour protéger les réseaux contre les attaques DDoS. Le logiciel inspecte l'adresse IP source de tous les paquets entrants, et s'il trouve une adresse IP qui représente plus de 1% du trafic global dans la dernière heure (la valeur de la période est paramétrable), il crée une règle dans le routeur pour bloquer tous les paquets provenant de cette adresse pour les prochaines 24 heures. Le directeur du marketing de TopSecurity affirme que cela peut contrer toutes les attaques DDoS distribuées.

a) Donner deux raisons pour lesquelles le logiciel de TopSecurity n'est pas une bonne solution à ce problème ?

a) Facile à casser : avec plus de 100 zombies, on peut inonder le lien réseau de la victime sans qu'aucun zombie consommant plus de 1 % du trafic.

Il est trop facile de changer l'adresse IP source de chaque paquet envoyé

b) Expliquer comment cette solution pourrait être mal utilisée (par un tiers malveillant) pour empêcher un utilisateur légitime d'accéder à un site Web protégé par ce logiciel.

en envoyant à la victime un grand nombre de paquets dont l'adresse IP source est celle du serveur innocent

Exercice 3 : Protocole « *Andrew Secure RPC* »

Le protocole *Andrew Secure RPC* est un **protocole de distribution de clef (symétrique)** reposant sur de la cryptographie symétrique. Plus précisément, le protocole doit garantir que :

- La nouvelle clef partagée (ci-dessous K'_{ab}) est secrète : dans chaque session la valeur de K'_{ab}, n'est connue que des participants jouant les rôles de *A* et de *B*.
- La nouvelle clef partagée K'_{ab} est **authentifiée** : dans chaque session, à la réception du message 4, *A* est assuré que la clef K'_{ab} obtenue dans le message a été créée par *B* lors de la même session.

Les hypothèses sont les suivantes :

- K_{ab} est une clef symétrique (pré-partagée) connue uniquement de *A* et de *B*.
- N_a et N_b sont des nombres pseudo-aléatoires.
- N'_b est un numéro de séquence initial qui sera utilisé dans une session future. **Ce paramètre ne joue aucun rôle dans cet exercice.**

Les messages du protocole sont les suivants :

1. A --> B : $A, \{N_a\}_{Kab}$
2. B --> A : $\{N_a+1, N_b\}_{Kab}$
3. A --> B : $\{N_b+1\}_{Kab}$
4. B --> A : $\{K'_{ab}, N'_b\}_{Kab}$

1. Expliquer brièvement le principe du protocole. En particulier :
   - Préciser son but
   - Dire si l'authentification est à sens unique ou mutuelle

- Justifier la réponse en explicitant la manière dont l'authentification est réalisée

  Protocole visant à distribuer une clé symétrique après authentification mutuelle des deux entités. L'authentification est du type défi-réponse, où chaque entité prouve sa connaissance de Kab en répondant au défi. Le « +1 » ajouté à Na et Nb dans les réponses a pour but de montrer que les entités ont vraiment réussi à déchiffrer Na (resp. Nb).

2. En remarquant que le message 4 ne comporte aucune information de fraîcheur (on suppose qu'aucune vérification sur N'_b n'est réalisée par *A*), exhiber un scénario très simple **d'attaque par rejeu**, où un intrus X réussit à faire accepter par *A* une clef symétrique K'_{ab} partagée lors d'une session précédente du protocole (et susceptible d'être compromise par X entre-temps).

   X observe une session entre A et B, et enregistre en particulier le message 4 qui contient K'ab. Lors d'une session ultérieure entre A et B, il interceptera le nouveau message 4 issu de B, et rejouera le message 4 qu'il avait enregistré. A acceptera alors à nouveau K'ab comme clé symétrique.

3. Proposez une modification du protocole permettant de contrer le scénario d'attaque précédent, n'utilisant pas de numéro de séquence ni d'estampille (« *time-stamp* »).

   4. B --> A : $\{K'_{ab}, \mathbf{Na}, N'_b\}_{Kab}$

4. M. Burrows, M. Abadi et R. Needham ont proposé une nouvelle version simplifiée comportant moins de chiffrement :

   1. A --> B : A, N_a
   2. B --> A : $\{N_a, K'_{ab}\}_{Kab}$
   3. A --> B : $\{N_a\}_{K'ab}$
   4. B --> A : N_b

   Le nonce Nb, envoyé dans le message 4, sera utilisé dans une session future.

   Proposez une attaque par entrelacement de sessions où un intrus peut se faire passer pour *B* auprès de *A*, i.e. à la fin du scénario d'attaque, *A* pense qu'il a établi une session avec *B* (l'intrus ne possédera pas pour autant la nouvelle clef de session).

   1. A --> X/B : A, N_a
   1'. X/B --> A : A, N_a
   2'. A --> X/B : $\{N_a, K'_{ab}\}_{Kab}$
   2. X/B --> A : $\{N_a, K'_{ab}\}_{Kab}$
   3. A --> X/B : $\{N_a\}_{K'ab}$
   3'. X/B --> A : $\{N_a\}_{K'ab}$
   4. X/B --> A : N_x
   4'. A --> X/B : N_b

5. Proposez une modification du message 2 permettant d'éviter l'attaque précédente.

   2. B --> A : $\{N_a, \mathbf{B}, K'_{ab}\}_{Kab}$

Partie 2 : Questions de cours (8 points)

Architectures et protocoles de sécurité

a. Dans le protocole SSL, expliquer comment les clés de chiffrement et de hachage (HMAC) sont-elles créées ?

Toutes ces clés dérivent de la clé maitre MSK qui est divisée en blocks : block1, block2, block3,…et chaque block sera utilisé comme clé pour hacher ou chiffrer. La MSK pourrait être modifié dans une session SSL.

b. Les attaques de déni de service ont des conséquences fatales et sont relativement faciles à mettre en œuvre. De nombreuses solutions ont été proposées pour résoudre le problème, mais elles sont toujours incomplètes. Quelles sont les limites de déploiement en termes de détection d'une part et de traçabilité d'autre part ?

Gestion isolée de la sécurité, distribution à l'échelle mondiale, problème de coopération entre les différents opérateurs, problèmes légaux, différenciation entre le trafic légitime et illégitime usurpation d'adresses, …

c. Peut-on retrouver la clé privé RSA à partir de la clé publique RSA ? Si oui, comment peut-on le faire ? Sinon, pourquoi ? Expliquer la réponse d'une manière détaillée.

Si on utilise des nombres premiers de petites tailles, oui, il est possible. On sait comment casser une clé de grande taille, mais c'est une question de temps de calcul….voire TD1

d. Proposer une mise en œuvre d'une attaque de l'homme en milieu dans un réseau local, en décrivant d'une manière détaillée l'ensemble des échanges entre les équipements (Faire une figure).

Exemple : ARP poisioning, ou autre

Voir le TD

e. Expliquer les conséquences des trois scénarios suivants en termes de sécurité :

1. Deux certificats différents sont signés par la même clef privée.

   Pas de problème. C'est le cas, quand une autorité de certification signe les certificats des serveurs web par exemple.

2. Deux certificats différents contiennent la même clef publique.

   Il y a un problème puisque deux personnes différentes possèdent les mêmes clés. Donc, chacun peut déchiffrer le message envoyé à l'autre….

3. Deux certificats différents ont la même signature.

   Collision au niveau de la fonction de hachage utilisée par l'AC

Réseaux sans fil et mobiles (pour les QCM, une seule bonne réponse par question, reporter SVP les réponses sur la copie d'examen. Il n'y a pas de pénalité en cas de mauvaise réponse.)

a. Comment la confidentialité des échanges est-elle assurée dans le protocole WEP ? Quelles sont les conséquences de la réutilisation du même vecteur d'initialisation dans deux trames différentes ?

WEP utilise une clé de 40 bits, elle est concaténée à un vecteur d'initialisation de 24 bits. La clé résultante sera utilisée pour chiffrer les données échangées en faisant simplement un XOR entre les données et la clé de 64 bits. Le vecteur IV est de taille 24 bits, il est transmis dans la trame en clair (pour qu'il soit utilisé par le récepteur). Si on

b. 802.1X est utilisé pour assurer :

- ☐ L'authentification
- ☐ L'intégrité
- ☐ La sécurité dans le GSM

c. L'AUc contient:

- ☐ Des informations sur l'abonné
- ☐ L'IMEI
- ☐ Le secret partagé entre l'opérateur et l'abonné

Tournez la page S.V.P.

d. Le contrôleur Wi-Fi:

- ☐ Permet une gestion centralisée du parc d'APs
- ☐ D'avoir des VPNs sur le réseau Wi-Fi
- ☐ Détecter les APs sauvages

Bon Courage.