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

Janvier 2016, *Durée 2h*

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

Exercice 1 : (Chiffrement / Déchiffrement RSA) – 3 points

Bob est le directeur des ressources humaines (RH) d'une entreprise. Il envoie le montant du salaire (en K€) d'un employé au PDG (Bernard) par email chiffré en RSA. La clef publique de Bob est (**e=11, n=55**) et celle de Bernard est (**e=5, n=51**). Une employée (Eve) intercepte ce mail et trouve le montant chiffré **C = 19**.

a) Calculer la clé privée correspondant à la clé publique du PDG.
N=p*q= 17*3 =51, phi=16*2=32
Par Bezout 5.d=1 mod 32 => d= 13

b) Quel est le salaire de l'employé en K€ ?
$M=C^d \bmod n = 19^{13} \bmod 51 = 49$ K€

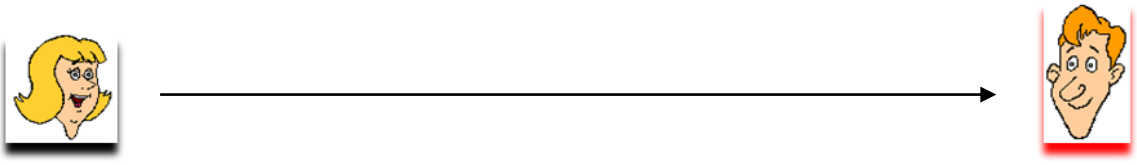
c) Est-il possible de chiffrer de longs messages avec RSA ? Justifier.
Très lourd. Pour des raisons de performance, on ne le fait pas. Théoriquement il est tout à fait possible de le faire.

Exercice 2 : (Services de sécurité) – 3 points

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*)
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 (**s_k n'est pas partagée au préalable**)
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. Rappelez ce qu'est une signature numérique, puis proposez une manière pour Alice d'envoyer son message afin d'assurer les propriétés de sécurité citées ci-dessus. Prenez en considération la présence d'Eve (attaque de MITM). **Vous justifierez votre solution en explicitant (rapidement) comment chaque propriété de sécurité est assurée**.



Alice Bob

Alice envoie les trois messages suivants :
C1=E K_B (s_k).
C2=E K^{-1}_A (Sha(M))
C3= AES_{sk} (M)

Bob déchiffre et vérifie

S_K=E K^{-1}_B (C1).
H=E K_A (C2))
M= AES_{sk} (C3)

Il hache h'= Sha (M) et il compare h avec h'.

Exemple d'un message échangé :

Si Alice souhaite chiffrer son message avec sa clé publique et l'envoyer avec un hash, elle transmettra par exemple : E_{KA}(M), SHA(M).

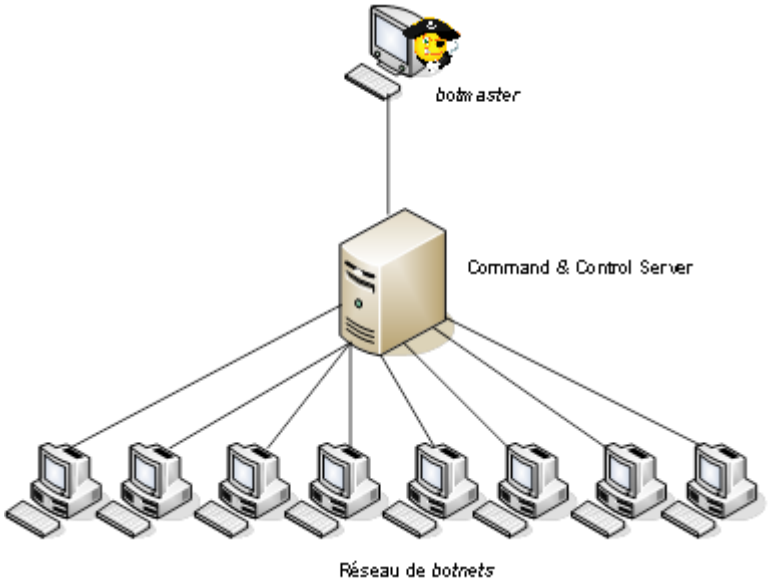
Exercice 3 : (Les botnets) (4 points)

Storm est sans nul doute l'un des plus connus sur la Toile et aussi l'un des plus dévastateur puisqu'il a comptabilisé jusqu'à 1,7 millions de machines infectées, un record pour un botnet ! Ce botnet a été dévastateur pour plusieurs raisons. Tout d'abord il a comptabilisé un très grand nombre de machines et il a aussi était le premier botnet à entièrement utilisé un réseau P2P pour fonctionner.

L'infection se fait de manière assez classique en envoyant un SPAM contenant une pièce jointe alléchante. Cette pièce jointe une fois exécutée installe alors un rootkit sur le poste de travail. Ce rootkit désactive les protections anti-virus et cache son processus. Ainsi, tout est fait de manière à ce que l'utilisateur ne se rende compte de rien.

Ce bot est très intelligent et c'est ce qui en a fait sa force. En effet, il refuse de s'exécuter au sein d'une machine virtuelle par exemple. De plus, le binaire principal du bot est chiffré empêchant ainsi de se faire détecter par un anti-virus. Le bot mute toutes les heures et son algorithme ainsi que sa clef de chiffrement change en même temps. Enfin, les serveurs de distribution du malware sont quasi impossible à détecter. Ce botnet fonctionne intégralement à l'aide du réseau P2P avec un mécanisme très complexe où tout est chiffré.

« *Hakin9* - 2010 »



Questions :

a. Quelles mesures faut-il prendre sur les postes clients pour éviter de faire partie d'un réseau de ce bot ?

Mise à jour de windows, anti spam, IDS à jour, plugin dans les navigateurs, anti malware, Firewall appli, etc. Un schéma avec les mesures de sécurité au niveau réseau et PC sera un plus.

b. Est-ce que la mise en place d'IDS/IPS sur le réseau local est suffisante ? Justifier votre réponse.
Non, il faut aussi des mesures de sécurité sur les machines. Sensibilisation à la sécurité, prendre des mesures de sécurité locales

c. Comment le botnet peut-il se propager ? Citez-différentes manières (3 minimum).
USB, spam, téléchargement des logiciels infectés sur les réseaux p2P, pièces jointes

Exercice 4 : Authentification (7 points)

Nous considérons dans cet exercice le protocole d'*authentification répétée* de Neuman Stubblebine. Il contient deux parties :

- une première dont le but est l'échange d'un *ticket*,
- une seconde, pouvant être répétée, dont le but est l'authentification à l'aide du ticket précédent.

Un déroulement du protocole fait intervenir trois entités *A, B* et *S* :

- les entités *A* et *B* essaient de s'authentifier mutuellement ;
- l'entité *S* est une entité de confiance générant les tickets.

Ce protocole utilise de la cryptographie symétrique. Les hypothèses sont les suivantes :

- *A* et *S* partagent une clef symétrique K_{AS} ;
- *B* et *S* partagent une clef symétrique K_{BS}.

Les messages de la première partie du protocole sont les suivants :

1. A --> B : A, r_A
2. B --> S : $B, r_B, \{A, r_A, t_B\}_{KBS}$
3. S --> A : $r_B, \{B, r_A, K_{AB}, t_B\}_{KAS}, \{A, K_{AB}, t_B\}_{KBS}$
4. A --> B : $\{A, K_{AB}, t_B\}_{KBS}, \{r_B\}_{KAB}$

La deuxième partie du protocole correspondant à l'authentification répétée est la suivante :

1. A --> B : r_A', $\{A, K_{AB}, t_B\}_{KBS}$
2. B --> A : r_B', $\{r_A'\}_{KAB}$
3. A --> B : $\{r_B'\}_{KAB}$

Les notations sont les suivantes:

- t_A et t_B désignent des estampilles,
- r_A, r_B, r_A', et r_B' désignent des nombres pseudo-aléatoires,
- K_{AS} et K_{BS} désignent des clefs symétriques (utilisées par un algorithme de chiffrement symétrique), partagées respectivement entre *A* et *S*, et entre *B* et *S*,
- K_{AB} une clef de session partagée entre *A* et *B* (utilisée par un algorithme de chiffrement symétrique).

1. Expliquez brièvement le principe du protocole (quelques lignes). En particulier :
   - Pour la première partie du protocole, précisez quel est le ticket partagé entre A et B, ainsi que le rôle de ce ticket dans le protocole.
   - Pour la deuxième partie du protocole, précisez comment A et B s'authentifient l'un à l'autre. (2 pts)

   Une attaque par *confusion de type* est une attaque portant sur la sémantique des champs d'un message. Il s'agit par exemple d'envoyer un nombre aléatoire à la place d'un identifiant. Si ces éléments ont la même longueur, et si le protocole ne vérifie pas le type des champs du message, le récepteur pourra interpréter le nombre aléatoire comme un identifiant.
2. On suppose que l'on ne vérifie pas le type des champs des messages et que r_A et K_{AB} sont de même longueur. Proposez une attaque par confusion de type sur la première partie du protocole, permettant à un attaquant *X* de se faire passer pour *A* auprès de *B* selon le squelette suivant : (1 pt)

   1. X/A --> B : ...
   2. B --> X/S : ...
   3. pas de message
   4. X/A --> B : ...

3. De même, en effectuant la même hypothèse que dans la question précédente, proposez une attaque par confusion de type sur la seconde partie du protocole prolongeant la précédente attaque, et permettant à un attaquant *X* de se faire passer pour *A* auprès de *B.* (1 pt)
4. On suppose que l'implémentation du protocole empêche des attaques par confusion de type. Proposez une attaque en sessions parallèles sur la seconde partie du protocole, selon le squelette suivant : (2 pts)

   1. X/A --> B : r_A', $\{A, K_{AB}, t_B\}_{KBS}$ *(message enregistré dans une session précédente)*
   2. B --> X/A : ...

   1'. X/A --> B : ...
   2'. B --> X/A : ...
   3. X/A --> B : ...

(les messages 1, 2 et 3 constituent une première session complète du protocole, les messages 1' et 2' correspondent eux à une seconde session incomplète du protocole).

5. Proposez une modification sur la seconde partie du protocole pour empêcher cette attaque. (1 pt)

Exercice 5 : Détection d'intrusion (3 points)

On souhaite configurer un IDS dans un système informatique afin de détecter l'attaque « Smurf ». On rappelle que cette attaque consiste à émettre une grande quantité de requêtes PING diffusées sur le réseau, tout en ayant pris soin de modifier l'adresse IP source des paquets afin qu'elle corresponde à l'adresse IP de la victime, qui se retrouve inondée de réponses. Le réseau considéré est 137.194.45.0/24.

1. Un HIDS peut-il être utile pour la détection de cette attaque ? Justifier. (1 pt)
2. On s'oriente sur une solution de type NIDS, telle que Snort. On commence par écrire la règle Snort suivante :

```
alert icmp any any -> 137.194.45.255 any (msg: "attaque Smurf"; sid:
10000002; rev: 1; itype: 8; icode: 0;)
```

   Expliquer brièvement ce que fait cette règle. (0,5 pt)

3. Quel problème pose la règle précédente pour la détection du Smurf ? Proposez une version améliorée de cette règle. Vous pouvez décrire cette modification avec vos propres mots, ou bien vous pouvez utiliser la syntaxe Snort pour écrire directement la règle modifiée (les erreurs de syntaxe ne seront pas pénalisées, du moment que la règle est compréhensible) (1,5 pt)

Bon Courage.