Master 2 Sciences Technologies
UNIVERSITE BORDEAUX 1 Sciences Technologies

ANNÉE 2011-2012 — SESSION DE DÉCEMBRE 2011

Étape : Master Sciences Technologies (semestre 3) — **UE :** MA9W03EX
Épreuve de : Sécurité des réseaux — **Durée :** 3h
Date : 15 Décembre 2011
Heure : 8h30
Documents documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer brièvement les différents modes de fonctionnement d'IPSec. Il vous est tout particulièrement demandé d'insister sur ce qui est chiffré et ce qui est en clair dans chacun des cas.
2. Expliquer brièvement le fonctionnement du protocole SSL/TLS. En quoi ce protocole est il différent d'IPSec ?
3. Expliquer brièvement ce qu'est une clé PGP et donner quelques exemples d'utilisation de ce genre d'objets. En quoi une clé PGP est différente d'un certificat X509 ?

Exercice 1

Un utilisateur qui a pour habitude d'utiliser la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? Lire le contenu (non-chiffré) des messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 2

Discuter les deux scénarios suivants en terme de sécurité :

1. Deux certificats sont signés par la même clé privée.
2. Deux certificats différents ont la même signature (i.e. même résultat après chiffrement du code de hachage). À quel genre de problèmes (de sécurité) cette situation peut-elle nous confronter ?

Exercice 3

Le protocole DHCP a pour objectif l'allocation des adresses IP de façon dynamique. DHCP fonctionne schématiquement de la manière suivante : lorsqu'une machine désire une adresse IP pour pouvoir se connecter à internet, elle envoie une requête DHCPDISCOVER à toutes les machines du réseau. Un serveur DHCP est alors chargé d'écouter sur ce réseau afin d'attribuer les adresses IP aux machines (le choix de l'adresse IP se fait à partir d'un ensemble d'adresses prédéfini). Lorsqu'il reçoit une demande, il retourne un paquet DHCPOFFER comportant une adresse IP assortie d'une période de validité ainsi que d'autres informations (telles que l'adresse de la passerelle ou du serveur DNS). Le serveur garde alors l'association entre l'adresse physique de la machine (MAC) et l'adresse IP qu'il lui a attribuée. Malheureusement, les échanges entre le serveur et les clients ne sont pas cryptées.

1. Décrire une attaque très simple qui permet à un pirate d'empêcher les clients d'obtenir une adresse IP. Proposer une solution simple qui permettrait au serveur d'éviter d'être complètement vulnérable face à cette attaque.
2. Comment est-il possible de compléter l'attaque précédente afin qu'un pirate soit capable d'intercepter les communications d'une machine cible ?

Exercice 4

On considère un système cryptographique à clef publique. Lorsque Alice veut envoyer un message secret à Bob, elle le crypte avec la clef publique de Bob et envoie en même temps à Bob un certificat qu'elle a elle-même fabriqué, contenant sa propre clef publique. Pour acquitter le message reçu, Bob renvoie le message à Alice, après l'avoir décrypté, puis ré-encrypté avec la clef publique qu'Alice lui a transmise dans son certificat.

1. Expliquer comment Oscar, pouvant espionner activement le réseau -man in the middle-, peut intercepter le message en clair.
2. En déduire le rôle des autorités de certification.
3. Comment éviter l'acte répréhensible d'Oscar sans passer par l'intermédiaire d'une autorité de certification ?

Exercice 5

Voici une variante du protocole de Needham and Schroeder vu en cours :

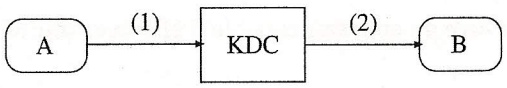
1. Alice $\rightarrow$ Bob : Alice
2. Bob $\rightarrow$ Alice : $\{\text{Alice}, \text{rand}_3\}_{k_{\text{Bob}}}$
3. Alice $\rightarrow$ Cathy : $\{\text{Alice}, \text{Bob}, \text{rand}_1, \{\text{Alice}, \text{rand}_3\}_{k_{\text{Bob}}}\}_{k_{\text{Alice}}}$
4. Cathy $\rightarrow$ Alice : $\{\text{Alice}, \text{Bob}, \text{rand}_1, k_{\text{session}}, \{\text{Alice}, \text{rand}_3, k_{\text{session}}\}_{k_{\text{Bob}}}\}_{k_{\text{Alice}}}$
5. Alice $\rightarrow$ Bob : $\{\text{Alice}, \text{rand}_3, k_{\text{session}}\}_{k_{\text{Bob}}}$
6. Bob $\rightarrow$ Alice : $\{\text{rand}_2\}_{k_{\text{session}}}$
7. Alice $\rightarrow$ Bob : $\{\text{rand}_2 - 1\}_{k_{\text{session}}}$

Cathy joue le rôle du serveur d'authentification. De plus, elle partage k_{Alice} (resp. k_{Bob}) avec Alice (resp. Bob).

Ce protocole est-il sensible aux attaques de type rejeu ? Expliquer.

Petit problème

Sur la figure suivante est présenté un protocole d'authentification utilisant un centre de distribution des clés (KDC). Dans ce schéma très simple, chaque utilisateur partage avec le KDC une et une seule clé. L'authentification et l'échange des clés de session entre deux utilisateurs se fait via le KDC.



Par exemple, si A veut communiquer avec B, il crée une clé de session K_{AB} et indique au KDC qu'il veut parler avec B en lui envoyant $\{A\}$ et $\{B, K_{AB}\}_{K_A}$ (message (1) sur la figure), où K_A est la clé partagée entre A et le KDC. Le KDC déchiffre alors ce message en construit un nouveau destiné à B contenant l'identité de A et la clé de session entre A et B. Ce message est chiffré avec la clé commune à B et au KDC : $\{A, K_{AB}\}_{K_B}$ (message (2) sur la figure). À partir de là, A peut envoyer des messages à B chiffrés avec K_{AB}.

1. Expliquer pourquoi un pirate ne peut pas se faire passer pour A auprès du KDC.
2. Expliquer pourquoi B est certain que le message provient bien du KDC.
3. À quelle attaque ce protocole ne résiste-t-il pas ?
   Aide : Supposons qu'un pirate I ait effectué un travail pour A. Après avoir échangé une clé de session via le KDC, A envoie un message à son banquier B pour lui demander de verser la rétribution sur le compte de I. Que faire à la place de I pour augmenter ses gains ?
4. Comment améliorer le protocole sans augmenter le nombre d'échanges pour déjouer ce type d'attaque ?

Problème

Le professeur de sécurité informatique est toujours très paranoïaque. Il doit partir en voyage à l'étranger or il n'a pas fini de préparer l'examen final pour son cours. Il doit donc envoyer le questionnaire de l'examen, une fois terminé, à sa secrétaire pour qu'elle puisse le vérifier et l'imprimer avant le jour de l'examen final. Comme il ne veut pas prendre le risque d'envoyer le questionnaire par courrier électronique (car il soupçonne que certains de ses étudiants en savent pas mal plus qu e lui en sécurité des réseaux), il décide d'utiliser PGP pour chiffrer le questionnaire avant de l'envoyer. Il utilise déjà PGP depuis un bon bout de temps. Sa clé publique est bien connue et réside déjà sur plusieurs serveurs de clés publiques. Son porte-clé (« key ring ») est déjà bien garni et contient les clés publiques de plusieurs amis, collègues et collaborateurs. Malheureusement, il remarque qu'il n'a pas la clé publique de sa secrétaire. Il lui envoie donc un courriel en lui expliquant ses intentions et la démarche à suivre, soit :

- elle installe GPG,
- elle génère une paire de clés privée et publique,
- elle lui envoie la clé publique par courriel,
- il chiffre le questionnaire avec la clé publique reçue et lui envoie le questionnaire chiffré et
- elle le déchiffre avec sa nouvelle clé privée.

1. Supposons qu'une étudiante soit au courant du plan du professeur, par exemple, parce qu'elle est capable d'intercepter (« sniffer ») tout le trafic qui se dirige et/ou sort du poste de la secrétaire à partir de son portable qui est branché sur le réseau de l'école, et elle est tombée sur le courriel

contenant les instructions envoyé par le professeur. Selon vous, est-ce que l'étudiante serait en mesure de se servir de tout ceci pour obtenir une copie du questionnaire avant l'examen ? Si oui comment, si non pourquoi ?

Remarque : l'étudiante n'est pas en mesure d'empêcher le trafic de se diriger vers sa destination .)

2. Le professeur, toujours très paranoïaque, ne croit pas une seconde à l'authenticité du courriel qu'il vient de recevoir de la secrétaire, contenant sa clé publique. En supposant, qu'il peut parler avec la secrétaire (par exemple, par téléphone), quel moyen peut-il utiliser pour vérifier l'authenticité non seulement du message reçu mais aussi de la clé publique reçue ?
3. Supposons maintenant que le professeur est dans un endroit tellement exotique qu'il ne peut pas entrer en communication avec sa secrétaire par téléphone. Il ne dispose que d'une connexion Internet de basse vitesse (donc pas de voix sur IP ou autre mécanisme multimédia). Quel autre moyen existerait-il pour qu'il puisse obtenir une copie de la clé publique de sa secrétaire dont il soit sûr de l'authenticité ?
4. Nous continuons exactement avec le même scénario que dans les questions précédentes. Cependant, dans ce cas ci le professeur décide d'utiliser une solution beaucoup plus simple. Il va tout simplement, se connecter sur le serveur Unix EXAMEN du département avec un tunnel SSH et utiliser une commande de copie de fichier qui utilise ce tunnel (tel que scp) pour copier le questionnaire sur dans répertoire auquel seulement sa secrétaire et lui ont accès. Pour se faire, un groupe d'utilisateur a été créé spécialement et les permissions sur ce répertoire sont telles que seuls les membres du groupe ont accès aux fichiers.

   (a) La même étudiante « hackeuse » continue à vouloir intercepter tout le trafic réseau qui se dirige et sort de la machine de la secrétaire, à partir de son portable qu'elle a connecté à une prise réseau dans un laboratoire. Sera-t-elle donc en mesure d'obtenir une copie de l'examen à temps ? Comment ?

   (b) Malheureusement pour l'étudiante, en réalité toutes les prises réseau des machines du personnel du département sont sur un VLAN (un sous-réseau virtuel de couche 2) différent de celui des laboratoires et différent de ceux des serveurs. De plus les switchs sont configurés de façon à ne rediffuser par défaut le trafic entre les différents VLAN qu'aux adresses MAC concernées. Quel type d'attaque de réseau l'étudiante pourrait-elle utiliser pour réussir quand même à intercepter les paquets entre la machine de la secrétaire et le serveur.