université de BORDEAUX

Master 1 *Sciences Technologies*

ANNÉE 2015-2016
Étape : Master Sciences Technologies (semestre 3)
Épreuve de : Sécurité des réseaux
Date : 16 Décembre 2015
Heure : 8h30

SESSION DE DÉCEMBRE 2015
UE : MA9W03EX
Durée : 1h30
Documents documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. 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 ?
2. 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.
3. Quel est l'intérêt de l'utilisation des *One-Time-Password*? Dans quel contexte ce genre d'objets sont-ils utilisés ? Donner un exemple d'utilisation de ce mécanisme.
4. L'une des caractéristiques du système d'authentification Kerberos est qu'un utilisateur n'a pas besoin de s'authentifier auprès du KDC chaque fois qu'il souhaite accéder à un service. Pourquoi ? Donner un avantage et un inconvénient (du point de vue de la sécurité) de cette caractéristique en les justifiant.

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 3

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

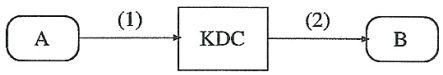
1. Alice $\rightarrow$ Bob : Alice
2. Bob $\rightarrow$ Alice : $\{\text{Alice}, \text{rand}_3\}_{k_{\text{Bob}}}$
3. Alice $\rightarrow$ Cathy : $\{\text{Alice}, \text{Bob}, \text{rand}_1, \{\text{Alice}, \text{rand}_3\}_{k_{\text{Bob}}}\}_{k_{\text{Alice}}}$
4. Cathy $\rightarrow$ Alice : $\{\text{Alice}, \text{Bob}, \text{rand}_1, k_{\text{session}}, \{\text{Alice}, \text{rand}_3, k_{\text{session}}\}_{k_{\text{Bob}}}\}_{k_{\text{Alice}}}$
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. Dans le cas où il le serait proposer une solution.

Exercice 4

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

Partie Irek Tobor

Durée : 1h30, 10 pts

Exercice 1, Questions de cours

1. On peut dire qu'une carte à puce est un ordinateur avec son jeu de composants (CPU, mémoire, circuits d'entrée/sortie, unités de calculs). Pourquoi dans les PC "de bureau" on a en général 2 types de mémoire (RAM et ROM) et dans les cartes à puces (et, en général, dans le domaine de l'embarqué) 3 (RAM, EEPROM et ROM) ? A quoi sert chacun de ces types de mémoire de la carte à puce et quel type de données est y stocké.
2. La communication entre un terminal et une carte à puce est faite en mode "maître-esclave" : c'est le terminal qui envoie la commande (APDU) et la carte qui doit répondre (R-APDU). Sauf un cas. Lequel ?
3. Pourquoi les cartes bancaires qui peuvent communiquer en mode "contact" et "sans contact" on ne peut pas toujours lire (dans le sens "c'est la spécification qui l'interdit") les mêmes informations (fichiers) dans ces deux modes.

Exercice 2, Authentification

L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une autre entité afin d'autoriser l'accès de cette entité à des ressources. L'authentification permet donc de valider l'authenticité de l'entité en question. Dans le cadre de cartes à puce la procédure d'authentification permet donc, par exemple de vérifier l'authenticité de la carte du point de vue du terminal ou l'inverse.

Plusieurs exemples peuvent se présenter :

1. Commande Internal Authenticate d'un protocole bancaire qui permet au terminal de s'assurer que la carte bancaire est authentique. La carte chiffre les données aléatoires envoyée par le terminal et le terminal vérifie si le chiffrement est correct.
2. Commande External Authenticate d'une autre application (par exemple du type IAS, dont on a pas parlé en cours) qui permet à la carte de s'assurer que le terminal qui lui envoie des commandes est authentique. Cette fois ci c'est le terminal qui doit chiffrer les données aléatoires envoyées par la carte et la carte à sont tour les vérifie.
3. Commande Mutual Authenticate du protocole GlobalPlatform qui est nécessaire avant le chargement d'une application / applet sur la carte. Elle permet de prouver mutuellement à la carte et au terminal que l'"autre" entité connaît bien les même clefs de chiffrement. Elle regroupe les deux cas précédents.
4. Procédure / protocole (pas une commande APDU !) Passive Authentication de passeport électronique. Elle consiste à vérifier la signature de différents fichiers du passeport (les données perso, la photo, etc). Cette signature est elle-même stockée sur la carte et on suppose que le terminal dispose de la clef publique nécessaire pour la vérifier. On suppose aussi que les fichiers de données et les signatures sont lisibles sans aucune procédure préalable, que la clef privée de signature n'est pas sur la carte et ne peut en aucun cas être trouvée et la clef publique est connue par terminal.
5. Procédure / protocole Active Authentication de passeport électronique. En plus des données personnelles la carte stocke la paire clef privée (pas lisible) et la clef publique. Terminal lit la clef publique, envoie des données à la puce qui les signe avec la clef privée et retourne cette signature. Le terminal peut donc la vérifier avec la clef publique qu'il a récupéré précédemment.

Notez que, pour les besoins de cet exercice, les hypothèses et les suppositions sont simplifiées par rapport aux cas réels. Il n'est pas demandé de donner la réponse exacte (un tel nombre d'octets, un tel format, plutôt des idées ou principes).