Composition de Sécurité logique et Edi-2002

La composition est décomposée en trois parties :

- Une partie théorique d'étude de certaines techniques de sécurité
- Une partie d'étude de cas
- Une analyse d'une attaque

Il est recommandé aux élèves de bien choisir l'ordre des parties selon leurs compétences et rapidités.

Le support de cours est permis.

1. Techniques de Sécurité (10 points)

Le protocole ETEBAC5 est un protocole de transfert sécurisé de fichiers.
L'implantation du protocole de transferts (PeSIT) utilise des verbes appelés des FPDU. (F-XXXXX)
L'implantation de la sécurité au niveau du protocole de transferts se fait en ajoutant des éléments de sécurité au niveau des verbes.
ETEBAC5 utilise des accréditations (pseudo-certificats) et sa propre API de sécurité.
Le but de cet exercice est d'étendre le protocole à l'utilisation des certificats X509, en utilisant PKCS11 comme API.

1.1 Implantation de la phase d'authentification mutuelle (8 points)

Phase	**Client**		**Serveur**
1- CONNEXION	Passage des paramètres identité	F-CONNECT ---------- >	• Vérification des identités
		F-CONNECT(ACK) < ----------	• Envoi de l'acquittement
2- CREATION FICHIER DISTANT	Demande de Création du Fichier distant et début de la phase d'authentification	F-CREATE ---------- >	• Création du fichier • Suite authentification
	…..	F-CREATE(ACK) < ----------	• Acquittement
3- OUVERTURE FICHIER DISTANT	Demande d'Ouverture du Fichier distant et suite de la phase d'authentification	F-OPEN ---------- >	• Ouverture du fichier • Suite authentification
		F-OPEN(ACK) < ----------	• Acquittement

L'authentification est implantée dans les phases 2 et 3.

a) Décrire les diverses mécanismes de l'authentification mutuelle côté client et serveur , les techniques de sécurité utilisées , ainsi que les paramètres de sécurité transmis avec chaque verbe. **(4 points, 15 lignes maximum)**

- Côté client avant la transmission de F-CREATE
- Côté serveur après la réception de F-CREATE et avant la transmission du F-CREATE(ACK)
- Côté client après la réception de F-CREATE(ACK) et avant la transmission du F-OPEN
- Côté serveur après la réception de F-OPEN et avant la transmission du F-OPEN(ACK)
- Côté client après la réception de F-OPEN(ACK)

b) Implanter les mécanismes d'authentification en utilisant les requêtes PKCS11 (usage des certificats d'authentification)**. (4 points).** Il n'est pas demandé d'implanter la vérification de la signature de l'autorité sur les certificats.

1.2 Analyse de la phase finale de transfert de données (2 points)

Phase	**Client**		**Serveur**
		F-WRITE ---------- >	
4- TRANSMISSION DE DONNEES	Transmission sécurisée des données Chiffrées et scellées	F-DATA ---------- >	• Déchiffrement des données reçues • Et scellement des données en clair
		F-DATA ---------- >	
		F-DATA ---------- >	
		…….	
		F-DATA ---------- >	
		F-DATA-END/F-TRANSEND ---------- >	
5- FIN DE TRANSMISSION DE DONNEES	Signature du client		• Vérification du la signature du client • Génération de l'accusé de réception
		F-TRANSEND(ACK) < ----------	
	Analyse de l'accusé de réception		• Acquittement
6- FERMETURE FICHIER DISTANT		F-CLOSE ---------- >	• Fermeture du fichier
	Demande de fermeture du Fichier distant.		
		F-CLOSE(ACK) < ----------	• Acquittement
7- LIBERATION FICHIER	Demande de libération du Fichier distant.	F-DESELECT ---------- >	• Libération du fichier
		F-DESLECT(ACK) < ----------	• Acquittement
8- DECONNEXION		F-RELEASE ---------- >	
		F-RELEASE(ACK) < ----------	

La norme précise que le transfert n'est considéré réalisé qu'à la réception par le client du F-DESELECT(ACK) deux phases plus loin que la réception de l'accusé de réception.

a) Démontrer que cette spécification de la norme est une faiblesse du protocole sécurisé de transfert de fichiers en décrivant une possibilité de litige.**(1 point, trois lignes)**
b) Que proposez vous pour éliminer cette faiblesse **(1point, trois lignes)**

2. Etude de Cas (10 points)

Une entreprise désire faire des virements avec sa banque au format EDIFACT/PAYMUL. La signature est basée sur l'utilisation du message AUTACK. Chaque fichier comporte deux signatures de 1024 bits. Il n'y a pas d'utilisation de certificats mais de clés nommées (chaque clé de signataire est définie par une identité unique). Chaque clé nommée est identifiée par un identifiant sur 35 octets.

1) Chaque signataire possède une carte à microcircuit pour signer. **(2 points).**
   - Définir le mapping de la carte (fichiers, types, droits d'accès, taille).
   - Deux cartes sont préconisées : 1Koctets et 4Koctets. Quelle est la carte qui doit être choisie ?

2) A cause de l'absence de certificats, le client envoie dans un message appelé KEYMAN, la liste des clés publiques avec leurs références. **(2 points, 4 lignes)**
   - Est ce que le message KEYMAN est suffisant?
   - Que proposez vous ?

3) La taille moyenne d'un virement unitaire est de 512 octets. Sachant que le message PAYMUL contient un enregistrement donneur d'ordre (512 octets), et 9999 virements unitaires en moyenne.

   - Quelle taille faut il prévoir pour l'enveloppe de sécurité avec deux signatures ? **(1 point)**
   - Calculer la taille moyenne d'un fichier signé. **(1 point)**

4) Le client a la possibilité entre trois solutions:
   - Achat d'un produit à 100000$ à la banque qui propose d'installer une passerelle de communication chez le client qui permet:
     - de vérifier les signatures du client sur la passerelle,
     - ôter les signatures AUTACK du fichier signé,
     - transmettre les fichiers sans signature AUTACK via un moyen de communication utilisant le PKCS7 comme enveloppe.
   - Achat d'un produit à 150000$ à une société qui permet la transmission par X400 des fichiers signés.
   - Développements en interne de quatre années-homme avec salaire annuel brut moyen de 30000$/ingénieur.

   a) Démontrer que la solution proposée par la banque ne doit pas être retenue en analysant les cas de litiges. **(1,5 point, trois lignes).**

   b) Quelle solution préconisez vous entre les solutions restantes? (**1 point**)

5) Les fichiers à signer sont fournis par un le système d'information du client selon un format SWIFT.
   a) Qu'est ce qu'il faut ajouter à l'architecture technique ? **(0,5 point 1 ligne)**
   b) Comment pouvoir authentifier d'une façon simple les fichiers provenant du système d'information ? **(1 point 2 lignes)**

3. Analyse d'une attaque (CHARGEN DENIAL OF SERVICE) – (2,5 points)

Un pirate analyse les ports de deux machines et détecte les services suivants actifs :

Machine 1 : d'adresse IP1

chargen (port = 19) sur udp

Machine 2 : d'adresse IP2

echo (port = 7) sur udp

Le service chargen permet de générer des caractères de nombre aléatoire vers le port et machine source.
Le service echo permet de ré-émettre les données qu'il reçoit vers le port et machine d'origine.

a) Décrivez la réaction au datagram UDP suivant : **(1 point)**

IP destinataire : IP1
port destinataire : 19
IP source : IP2
port source : 7

b) Qu'est ce qui résulte de l'envoi de plusieurs datagrams du type précédent. **(1 point)**

c) Que préconisez vous pour empêcher le résultat en b ? **(0,5 point)**