Composition de Sécurité logique - 2004

La composition est décomposée en trois parties :

?? Une partie d'étude de cas
?? L'utilisation d'une API de sécurité
?? Une partie théorique d'étude de certaines techniques de sécurité

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

Le support de cours est permis. La majeure partie des questions font appel au sens pratique d'ingénieur et le suivi du cours en classe, il est recommandé à l'élève de ne pas perdre son temps pour rechercher les solutions dans le support de cours.

1. Etude de Cas Réel (6 points)

Swift est un réseau mondial permettant l'interconnexion des banques pour l'échange des données entre elles. Swift compte élargir son offre pour la connexion des entreprises aux banques avec une implémentation d'une PKI autour d'une autorité de certification gérée par Swift. La connexion à Swift est faite par une liaison spécialisée déployée chez l'entreprise. Le transfert des données se fait avec utilisation d'une signature et le chiffrement des données.
Deux modes d'échanges de données sont supportées :

?? Mode Swift natif où les données sont au format unique Swift et nécessite l'utilisation d'une station Swift.
?? Mode FileAct où les données transmises par l'entrepris e peuvent être de format quelconque.

a) Citer un avantage concernant l'échange des données lors de l'utilisation du mode Swift Natif (1 ligne)
b) Citer deux avantages (échange des données et sécurité) pour l'utilisation du mode FileAct (3 lignes)
c) Une petite entreprise veut échanger les données avec une banque via Swift. Pour quelle raison est il intéressant que l'entreprise utilise des certificats Swift ? (2 lignes)
d) Une grande entreprise possède déjà des certificats délivrés par une autorité tierce.
    i. Est ce que les certificats délivrés par Swift sont nécessaires ?
    ii. Dans le cas où l'entreprise utilise ses propres certificats comment les banques destinatrices et possédant des certificats Swift peuvent gérer les signatures de l'entreprise ?
e) Chaque signataire possède une carte à puce sur laquelle existent 4 certificats et 4 clés privées ainsi que le certificat de l'autorité . Nous supposons l'utilisation du RSA 1024 bits.
    i. Ecrire le mapping de la carte à puce.
    ii. Quelle carte utiliser parmi les cartes suivantes (1Koctets, 8 Koctets, 64Koctets).

2. API de sécurité (6 points)

Le but de cet exercice est d'implémenter les services de non répudiation en utilisant les requêtes de sécurité Etebac5. Soit un fichier qu'il faut transmettre d'un client à sa banque en clair.

a) Décrire les mécanismes de signature du client et de vérification de signature par la banque.
b) Implémenter la signature en utilisant les requêtes de sécurité Etebac5. (ne pas inclure les requêtes d'accès au dispositif)
c) Implémenter la vérification signature en utilisant les requêtes de sécurité Etebac5. (ne pas inclure les requêtes d'accès au dispositif).

3. Analyse du Chiffrement en mode CBC (14 points)

Le but de cet exercice est d'analyser une éventuelle attaque par couple (données en clair connues, données chiffrées) sur le dernier bloc de données dans le cas d'un algorithme symétrique en mode CBC.
Une partie de la notation de cette partie tient compte de la bonne capacité de l'élève à analyser le problème. Certaines parties sont simples, d'autres difficiles.
Dans la suite d'exercice on suppose les notations suivantes :

Le document en clair est constitué de blocs de données $B_0B_1…..B_i…B_{n-1}B_n$,
Le document chiffré est constitué de blocs de données $B'_0B'_1…..B'_i…B'_{n-1}B'_n$, ,
B_0, B'_0 : premiers blocs de données en clair et chiffrés, chacun de 8 octets
Bi, B'i : blocs de données d'ordre i en clair et chiffrés, chacun de 8 octets
B_{n-1}, B'_{n-1} : avant dernier blocs en clair et chiffrés, chacun de 8 octets
B_n, B'_n : derniers bloc en clair et chiffrés chacun de 8 octets.
IV: vecteur d'initialisation
K : clé de chiffrement symétrique
F : algorithme de chiffrement symétrique,
Pn : padding du dernier bloc réalisé par une fonction de padding P

3.1 Ecriture des équations(2 points)

a) Ecrire la relation qui lie : B_0, B'_0, IV, F,K.
b) Ecrire la relation qui lie : B_i, B'_i, B'_{i-1} , F,K.
c) Ecrire la relation qui lie : B_n, B'_n, B'_{n-1} , F,K, Pn
d) Décrire l'attaque par couple (données en clair connues, données chiffrées). (2 Lignes)

3.2 Analyse dans le cadre d'un fichier de format variable (5 points)

On appelle un fichier de format variable un fichier dont la structure et le format utilisent des enregistrements de taille variable (exemple : Edifact, Swift).
Considérons le cas d'Edifact dont le dernier enregistrement (segment) est de la forme UNZ+1+ABCDEF'
Supposons que le dernier bloc à chiffrer soit connu, de taille connue et qu'il ait la valeur: EF' .

a) Dans le cadre d'un padding par des 0 binaires, est ce que le dernier bloc peut être attaqué par l'attaque de couple ?
b) Dans le cadre d'un padding par des valeurs aléatoires, supposons qu'en décryptant on a une valeur de clé Kd donnant EF'abcde. (où abcde sont des valeurs binaires quelconques).
    a. Démontrer qu'ils existent d'autres valeurs de clés donnant une donnée en clair de ce format.
    b. Quelle est le nombre de ces clés ?
    c. Comment arriver à découvrir la bonne valeur de la clé ?
c) Nous avons supposé que le dernier segment en clair a une valeur connue UNZ+1+ABCDEF'. Or ABCDEF constitue la référence de l'interchange Edifact et donc est variable et non connu en avance.
    a. Quelle est dans ce cas la seule partie des données en clair connue et entrant dans le dernier bloc ?
    b. Conclure sur la résistance du format Edifact contre l'attaque en question. (Prendre en compte tous les facteurs).

3.3 Analyse dans le cadre d'un fichier de format fixe(4 points)

On appelle un fichier de format fixe un fichier dont la structure et le format utilisent des enregistrements de taille fixe (exemple : formats français, espagnols,…).
Considérons le cas d'AFB320 (virement international français) dont l'enregistrement a une taille de 320 octets.
Le dernier enregistrement en AFB320 a la structure suivante :

Zone	**Nom**	**Longueur**	**Commentaires**
1	Code Enregistrement	2	Valeur = '08'
2	Code Opération	2	Valeur = 'PI'
3	Numéro séquentiel	6	Numéro enregistrement précédent incrémenté de 1
4	Date de Création	8	
5	Zone réservée	4*35	A blanc
6	Siret de l'émetteur	14	Identifiant client
7	Référence	16	
8	Zone réservée	11	A blanc
9	Type du compte donneur d'ordre	1	
10	Numéro du compte donneur d'ordre	34	
11	Code devise	3	
12	Nom client	34	
13	Total de contrôle	18	Somme de touts les montants du fichier
14	Zone réservée	49	A Blanc

a) Dans le cadre d'un padding par des 0 binaires quel est le dernier bloc en clair connu qu'il faut utiliser pour l'attaque? (1 ligne)
b) Dans le cadre d'un padding par des valeurs aléatoires quel est le dernier bloc en clair connu qu'il faut utiliser pour l'attaque? (1 ligne)
c) Que proposer au niveau des zones 4,8 et 14 pour renforcer la résistance de l'AFB320 contre l'attaque ?
d) En modifiant les zones 4,8 et 14 est ce que c'est suffisant ?
e) Conclure sur la résistance du format AFB320 contre l'attaque en question. (Prendre en compte tous les facteurs).

3.4 Conclusions(3 points)

a) Conclure sur l'attaque sur dernier bloc selon les formats, les paddings, ….
b) Nous avons supposé que les fichiers en clair ne sont pas pré-traités avant chiffrement. Que proposez vous comme opération supplémentaire avant chiffrement pour se protéger contre l'attaque.