M1 informatique - UE réseau et sécurité

Année universitaire : 2018-2019

Consignes : documents interdits, calculatrices interdites, téléphones portables interdits.

Examen terminal – première session

Exercice 1 : Cryptanalyse du chiffrement de Vigenère (5 points)

La méthode du mot probable est une des techniques pour cryptanalyser le chiffrement de Vigenère.

Question 1.1 (1 point) : Comment fonctionne la méthode du mot probable ?

Question 1.2 (1 point) : Que se passe-t'il si le mot probable est court ?

Question 1.3 (1 point) : Que se passe-t'il si le mot probable a une longueur de k+1, avec k la longueur de la clé ? Quelle est la bonne taille du mot probable ?

Question 1.4 (1 point) : Que se passe-t'il si le mot probable n'apparaît pas dans le texte ?

Question 1.5 (1 point) : Comment concevoir un chiffrement basé sur Vigenère qui empêche la technique du mot probable ?

Exercice 2 : Signatures (4 points)

Question 2.1 (1 point) : Rappelez comment on produit la signature S d'un message M.

Question 2.2 (1 point) : Rappelez comment on vérifie la signature S d'un message M.

Question 2.3 (1 point) : Supposons qu'il est possible de créer une collision d'une fonction de hachage sur un message M (c'est-à-dire, on peut trouver M' tel que $H(M')=H(M)$). Prouvez l'impact sur le mécanisme de signature.

Question 2.4 (1 point) : Est-il possible de créer des collisions d'une fonction de hachage sur un message M ? Est-ce difficile ?

Exercice 3 : Attaque Chop-chop sur WEP (11 points)

WEP (Wired Equivalent Privacy) [1] est un protocole de sécurité pour les réseaux sans fil, qui n'a pas été étudié en cours. Ce protocole a été rendu obsolète en 2004 à cause de problèmes de sécurité. Dans cet exercice, nous allons discuter de l'attaque Chop-chop [2] sur WEP. Dans la suite, $||$ représentera la concaténation de deux messages binaires et $+$ représentera le XOR de deux messages binaires. $\{M\}_K$ dénotera le chiffrement avec un XOR de M en utilisant la clé K, c'est-à-dire $\{M\}_K=M+K=\{M\}_K^{-1}$.

Supposons qu'un client et un point d'accès communiquent ensemble. Le client et le point d'accès partagent une clé primaire Rk. Pour transmettre un message M, le client génère tout d'abord un nombre aléatoire IV (pour *initialization vector*), et calcule $K=RC4(IV||Rk)$ avec le chiffrement par flux RC4. Ensuite, le client calcule $C=\{M||ICV\}_K$, où ICV (pour *integrity check value*) est une somme de contrôle de 32 bits correspondant à M, obtenue par l'algorithme du CRC32. Finalement, le client envoie $IV||C$ au point d'accès. Quand le point d'accès reçoit $IV||C$, il en extrait le message et le ICV. Si le ICV est correct, le point d'accès retransmet le message. Sinon, le message est ignoré. Nous faisons l'hypothèse que l'attaquant peut intercepter tous les messages transmis par le client ou par le point d'accès.

Question 3.1 (0.5 point) : Quel est le principal service de sécurité fourni par WEP ?

Question 3.2 (0.5 point) : Quelle est la taille de la clé K ? Pour répondre, utilisez le fait que $C=\{M||ICV\}_K$.

Question 3.3 (0.5 point) : À quoi sert IV ?

Question 3.4 (0.5 point) : À quoi sert ICV ?

Question 3.5 (1 point) : Expliquez comment le point d'accès est capable d'obtenir le message initial à partir de $IV||C$, et de vérifier son intégrité. Est-ce que RC4 est un algorithme symétrique ou asymétrique, en vous basant sur cette description ?

L'algorithme du CRC32 considère les messages binaires comme des polynômes (par exemple, $1101=x^3+x^2+1$), et se base sur la division polynomiale. Selon l'algorithme du CRC32, $ICV=M.x^{32}$ $[R]$, pour un polynôme donné R.

Question 3.6 (1 point) : Montrez que $\{C\}_K^{-1}=0$ $[R]$.

L'attaque Chop-chop est une attaque itérative qui consiste (1) à enlever le dernier octet de C pour générer un nouveau message A (c'est-à-dire, $C=A||B$, avec B sur un octet), (2) à transformer le message A en un message $A'=A+x^{-8}D$ en devinant la valeur non-chiffrée D de l'octet supprimé B, et (3) à vérifier si la somme de contrôle de A' est correcte ou non en écoutant la retransmission de la trame A' par le point d'accès.

Question 3.7 (2 points) : Pour s'assurer que la somme de contrôle du message A' est correcte, le point d'accès détermine si $\{A'\}_{K1}=0$ $[R]$ ou pas (voir question 3.6), où $K1$ est égal à K sans son dernier octet. Montrez que si D est connu, la somme de contrôle de A' sera correcte.

Question 3.8 (1 point) : Expliquez comment deviner la valeur D.

Question 3.9 (1 point) : Expliquez l'attaque complète, permettant d'obtenir le message en clair correspondant au message complet M (et pas seulement le dernier octet).

Question 3.10 (1 point) : Dans cette attaque, combien de trames réelles sont capturées ? Combien de trames forgées sont envoyées ?

Question 3.11 (1 point) : Est-ce que l'attaquant est capable d'obtenir K ? Est-ce que l'attaquant est capable d'obtenir Rk ?

Question 3.12 (1 point) : Proposez deux manières d'éviter cette attaque.

Références

[1] IEEE Std 802.11-1997. “Telecommunications and information exchange between systems - local and metropolitan area networks-specific requirements, part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications”. 1997.

[2] Korek. “Chop-chop experimental WEP attacks”, published on http://www.netstumbler.org/. 2014.