M1 informatique – UE réseau et sécurité – deuxième session

Année universitaire : 2023-2024

Consignes : documents interdits, calculatrices et téléphones portables interdits.

Exercice 1 : Cryptanalyse différentielle (5 points)

Considérons tout d'abord le chiffrement de Vigenère.

Question 1.1 (2 points) : Notons K la clé, et n la taille de K en bits. Rappelons que le chiffré C d'un message clair M est obtenu grâce à C[i]=M[i]+K[i%n], où « + » représente l'opération XOR, et « % » représente l'opération modulo. Considérons qu'un attaquant connaisse un message M1 et son chiffré C1, et souhaite chiffrer un message M2 (de longueur inférieure ou égale à M1). Montrez comment l'attaquant peut calculer le chiffré C2 de M2. Pour cela, vous pourrez vous inspirer de la cryptanalyse différentielle en exprimant la différence des chiffrés en fonction de la différence des messages clairs.

Considérons à présent la cryptanalyse différentielle d'une version légèrement modifiée du protocole DES, dans laquelle le nombre de tours est un paramètre, et sans les permutations initiales et finales.

Question 1.2 (1 point) : Quand le nombre de tours est 1 ou 2, il existe un algorithme qui permet de réduire grandement l'espace des clés possibles à partir de deux messages aléatoires M1 et M2, et des deux chiffrés correspondants C1 et C2. Mais, pour un couple donné, cet algorithme ne permet pas nécessairement de trouver une seule clé possible. Comment réduire l'espace des clés à une unique valeur, et ainsi trouver la clé utilisée ?

Question 1.3 (2 points) : Quand le nombre de tours est supérieur ou égal à 3, il existe un algorithme probabiliste qui essaye de deviner la clé en générant un très grand nombre de couples de messages aléatoires, et en observant pour chaque couple les écarts des différences des couples de chiffrés. Expliquez cet algorithme probabiliste. Vous pouvez utiliser un schéma pour appuyer votre explication.

Exercice 2 : Protocole DoH (4 points)

Le protocole DoH (DNS over HTTPS) [1] est une alternative à l'usage du protocole DNS classique, plus respectueuse de la vie privée. Dans DoH, un client qui souhaite obtenir une adresse IP se connecte en HTTPS à un résolveur intermédiaire, lui transmet sa requête chiffrée, et c'est le résolveur intermédiaire qui effectue la résolution DNS.

Question 2.1 (1 point) : Détaillez la manière dont un utilisateur peut obtenir l'adresse IP d'un serveur, avec le DNS classique.

Question 2.2 (1 point) : Avec le DNS classique, est-ce qu'il est possible pour quelqu'un observant le trafic d'un utilisateur de connaître les serveurs dont l'utilisateur demande la résolution de noms ? Pourquoi ?

Question 2.3 (1 point) : Avec DoH, est-ce qu'il est possible pour quelqu'un observant le trafic d'un utilisateur de connaître les serveurs dont l'utilisateur demande la résolution de noms ? Pourquoi ?

Question 2.4 (1 point) : En quoi la propriété de respect de la vie privée de DoH est liée à l'hypothèse d'un grand nombre de résolveurs DoH intermédiaires ?

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

WEP (Wired Equivalent Privacy) [2] 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 [3] 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 (1 point) : Quel est le principal service de sécurité fourni par WEP ?

Question 3.2 (1 point) : Quelle est la taille de la clé K ? Pour répondre, utilisez le fait que $C=\{M||ICV\}_K$.

Question 3.3 (1 point) : À quoi servent IV et ICV ?

Question 3.4 (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.

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 3.5 (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 3.6 (1 point) : 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 3.5), où K1 est égal à K sans son dernier octet. Montrez que si D est connu, A' sera correcte.

Question 3.7 (1 point) : Expliquez comment deviner la valeur D.

Question 3.8 (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 3.9 (1 point) : Dans cette attaque, combien de trames réelles sont capturées ? Combien de trames forgées sont envoyées ?

Question 3.10 (1 point) : Est-ce que l'attaquant est capable d'obtenir K ? Est-ce que l'attaquant est capable d'obtenir Rk ?

Question 3.11 (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.

[3] Y. Qiu, B. Li, Z. Li, L. Jiao, Y. Zhu, Q. Liu. “Before toasters rise up: A view into the emerging DoH resolver’s deployment risk,” work in progress, 2023.