MASTER COMASIC

TD Vulnérabilités

Jean Leneutre

CORRECTION EXERCICE (Sécurité WEP)

1- On peut relever les défauts suivants :

i. L'authentification n'est pas mutuelle.

ii. L'authentification et le mécanisme de chiffrement pour la confidentialité utilisent la même clef.

iii. STA n'est authentifié que seulement au moment où il se connecte au réseau : une fois que STA est authentifié, n'importe qui peut envoyer des messages en se faisant passer pour STA en « spoofant » l'adresse MAC de STA. C'est un réel problème si les différentes STA utilisent la même clef.

2 Soit S la séquence pseudo-aléatoire. L'attaquant peut capturer deux messages chiffrés : $m \oplus S$, et $m' \oplus S$. L'attaquant peut alors calculer : $m \oplus S \oplus m' \oplus S = m \oplus m'$. Cela revient à un message en clair chiffré avec un autre. Mais des messages en clair n'ont pas les propriétés des séquences pseudo-aléatoires.

Si l'attaquant connaît déjà un des deux messages, il peut déduire l'autre.

Sinon, l'attaquant peut utiliser les propriétés statistiques des messages en clair. Par ailleurs, l certaines parties fixes des messages (headers, ...) peuvent être connues, ce qui peut faciliter le travail de l'attaquant. Par exemple, sachant que la majorité du trafic d'un réseau Wi-Fi est constitué de trafic IP, on peut déduire ce que contiennent les headers des trames. On peut notamment identifier les paquets ARP par leur taille et leur adresse de destination qui est l'adresse broadcast Ethernet (FF :FF :FF :FF). On peut ensuite connaître la structure et les valeurs courantes de certains champs des paquets ARP (8 octets d'en-tête LLC/SNAP, 8 octets d'en-tête ARP, 6 octets d'adresse MAC de la source). Le fait de disposer de toutes ces informations permet de retrouver avec une forte probabilité les premiers octets du « keystream » (22 pour un paquet ARP, 8 pour un paquet IP) et progressivement la totalité du key stream. Ce type d'attaque est dénommée « attaque par clé apparentée » ou encore « attaque active des extrémités ».

3-a Du fait de la méthode de chiffrement utilisée un attaquant X peut se faire passer pour STA auprès de AP (sans connaître pour autant la clef k) :

- *l'attaquant X écoute une session d'authentification entre STA et AP*

  $STA \rightarrow AP : \quad STA$

  $AP \rightarrow STA : \quad r_{AP}$

  $STA \rightarrow AP : \quad IV, \ (r_{AP}, AP) \oplus RC4(k||IV)$

- *X calcule* $RC4(k||IV) = ((r_{AP}, AP) \oplus RC4(k||IV)) \oplus (r_{AP}, AP)$

- *ensuite X redémarre une nouvelle session en se faisant passer pour STA en utilisant le même IV et donc la même séquence aléatoire :*

  $X/STA \rightarrow AP : \quad STA$

  $AP \rightarrow X/STA : \quad r_{AP'}$

  $X/STA \rightarrow AP : \quad IV, \ (r_{AP'}, AP) \oplus RC4(k||IV)$

3-b- 8Mbit=1 million d'octets. En 1s, 1000 valeurs IVs sont utilisées. Il faut attendre 17 000 s, soit environ 4 H45mn.

Il suffit pour l'attaquant de stocker la valeur de $m \oplus S$ pour chaque IV. Puis quand le même IV est réutilisé pour chiffrer un message m', l'attaquant peut calculer $m \oplus m'$, et se retrouve dans le cas de la question 2-a. Ensuite, une fois qu'il a retrouvé m et m', il peut calculer S et l'inclure dans la table.

Concrètement, pour réaliser cette attaque l'attaquant doit capturer et analyser les trames. Pour cela l'attaquant écoute (« sniffe ») le réseau en mettant la carte Wi-Fi en mode « monitor » : la carte ne se comporte plus comme une interface réseau normal mais capture tout le trafic dans le voisinage. Il peut utiliser ensuite un analyseur de protocole comme ETHEREAL, KISMET ou encore WIRESHARK.

3-c Le vecteur IV étant sans cesse renouvelé, une valeur faible va finir par apparaître (dans la pratique au bout de quelques milliers de messages). Il suffit pour l'attaquant d'espionner le trafic jusqu'à ce qu'il repère une valeur faible. Il peut alors deviner la racine, et récupérer k.
Comme cette attaque permet de calculer directement la clef k, elle ne nécessite pas d'espace mémoire pour stocker toutes les valeurs de séquences pour chaque IV.

4-a *Soit ΔM, le changement que l'attaquant veuille faire dans M.*

L'attaquant doit construire (M⊕ ΔM || CRC(M⊕ ΔM))⊕ S à partir de (M || CRC(M))⊕ S
Il suffit pour cela qu'il calcule ΔM || CRC(ΔM), car :
[(M || CRC(M))⊕ S] ⊕ (ΔM || CRC(ΔM))= (M⊕ ΔM || CRC(M)⊕ CRC(ΔM))⊕ S)= (M⊕ ΔM || CRC(M ⊕ ΔM))⊕ S

4-b Soit (M || CRC(M))⊕ S le paquet IP chiffré dont l'attaquant connaît l'adresse IP de destination. Il peut calculer le ΔM permettant de remplacer l'adresse de destination de M par celle de l'hôte qu'il contrôle.
D'après la question précédente, il peut reconstruire un paquet IP chiffré correct en calculant :
[(M || CRC(M))⊕ S] ⊕ (ΔM || CRC(ΔM))

Il lui suffit ensuite de renvoyer ce paquet IP modifié à l'AP. L'AP va déchiffrer le contenu de ce paquet et l'envoyer à la passerelle reliée à Internet, qui à son tour le renverra vers l'attaquant. Ce type d'attaque s'appelle une « Redirection IP » (ou « IP Forwarding »).

Commentaire :
Dans le cas où le réseau n'est pas relié à Internet il existe une autre attaque permettant de déchiffrer le trafic TCP/IP en utilisant l'AP pour déchiffrer la trame. Cette attaque consiste à forger des messages et à tester les réactions du destinataire selon qu'il l'accepte en renvoyant un accusé de réception (ACK) ou non, en la rejetant (le destinataire est qualifié d'oracle). Selon la réaction (qui dépend de la validité du TCP Checksum), l'attaquant pourra déduire des octets du plaintext.

5- *De possibles améliorations sont :*

- *augmenter la taille de l'IV (complexifie l'attaque de la question 2-b).*
- *calculer la valeur racine de RC4 comme une fonction de k et IV et non comme une simple concaténation de k et IV (complexifie l'attaque de la question 2-c).*
- *renouveler la clef k.*
- *modifier la fonction de vérification d'intégrité du message (empêche l'attaque de la question 3).*

Le protocole TKIP (« Temporal Key Integrity Protocol ») de la norme WPA a intégré certaines de ces améliorations. La norme WPA2 remplace quant à elle l'algorithme RC4 par AES.

CORRECTION EXERCICE (Sécurité RC4)

6- *On obtient le tableau suivant (K_0=3, K_1=255 et K_2=X), dans le cas où $5+X \leq 255$ et $6+X+K_3 \leq 255$:*

Vecteur P	*0*	*1*	*2*	*3*	*4*	...	*5+X*	...	*6+X+K_3*	...
Initialisation	*0*	*1*	*2*	*3*	*4*	...	*5+X*	...	*6+X+K_3*	...
i=0,j=0+P_0+K_0=3	*3*	*1*	*2*	*0*	*4*	...	*5+X*	...	*6+X+ K_3*	...
i=1, j=3+P_1+K_1=3+1+255=3	*3*	*0*	*2*	*1*	*4*	...	*5+X*	...	*6+X+ K_3*	...
i=2, j=3+ P_2+K_2=3+2+X=5+X	*3*	*0*	*5+X*	*1*	*4*	...	*2*	...	*6+X+ K_3*	...
i=3, j=5+X+ P_3+K_3=6+X+K_3	*3*	*0*	*5+X*	*6+X+ K_3*	*4*	...	*2*	...	*1*	...

7- *On a i=1 et j=0+ P_1=0, P_0 devient 0 et P_1 devient 3, donc le nouvel octet O= P_3=6+X+ K_3 mod 256.*

8- *Si un attaquant récupère un message chiffré m⊕S, avec un IV de la forme K_0=3, K_1=25 et K_2=X, et connaît le premier octet de m, alors il peut obtenir le premier octet O de S, et déduire K_3 :*

K_3=O-6-X mod 256.

9- *Les valeurs de P_0, P_1, P_3 ne sont plus impactées par la variable i dans l'algorithme de génération de la suite pseudo-aléatoire car i>3 à l'issue de la quatrième itération. Ces valeurs ne seront pas impactées si j est différent de 0, 1 ou 3 pendant les 252 itérations de l'algorithme de génération de la permutation. En supposant que les valeurs affectées à j soient aléatoires (c'est une approximation raisonnable), la probabilité que les valeurs de P_0, P_1, P_3 restent identiques pendant les 252 itérations restantes est :*

$(253/256)^{252} \approx 0,0513$

10- *Si l'attaquant connaît K_3, alors s'il observe un vecteur IV tel que K_0=4, K_1=255 et K_2=X, il peut espérer trouver K_4=O-10-X mod 256.*

CORRECTION EXERCICE (Sécurité WPA2)

1- La station installe la clef PTK dans l'état PTK-DONE. Le message 1 peut-être retransmis par l'AP alors que la station est dans l'état PTK-START ou dans l'état PTK-DONE (dans le cas où l'AP n'a pas reçu le message 4 du protocole d'authentification)Le message 3 peut-être retransmis par l'AP alors que la station est dans l'état PTK-DONE (dans le cas où l'AP n'a pas reçu le message 4 du protocole d'authentification). Dans ce cas le nonce utilisé par l'algorithme de chiffrement CCMP (ou GCMP) est initialisé de nouveau à 0.

2- Il suffit pour l'attaquant de bloquer le message 4 : la station va passer dans l'état PTK-DONE et va commencer à émettre des paquets de données chiffrées (en utilisant le protocole 802.1X). L'AP ne recevant pas de message 4 va réémettre le message 3. À sa réception la station réinitialise le nonce de chiffrement à 0, et réémet le message. Les prochains chiffrements de données réutiliseront potentiellement des nonces déjà utilisés.