MASTER COMASIC

TD Vulnérabilités

Jean Leneutre

CORRECTION EXERCICE (Sécurité WEP)

1-a On souhaite assurer la confidentialité entre STA et AP de l'information contenue dans les messages échangés lors de la session de communication. En fait, on verra dans la question 4 que l'on souhaite également l'intégité de ces informations (aucune modification). Cela présuppose également d'assurer la confidentialité et l'intégrité de la clef k.

1-b A la réception du message M_3, AP déchiffre le message avec k, vérifie que l'identifiant AP est correct, puis que le nombre pseudo-aléatoire est bien celui qui a été envoyé dans le message M_2. Si c'est le cas, en supposant que r_{AP} n'a jamais été utilisé dans une exécution passée du protocole, AP a la garantie que le message M_3 vient d'être construit et envoyé par une entité connaissant k. AP est donc assuré d'interagir avec STA.

1-c Non, c'est un protocole d'authentification unilatéral et non mutuel.

1-d Si l'attaquant récupère la clef k :

- *L'attaquant peut se faire passer pour STA*
- *L'attaquant peut déchiffrer toutes les sessions de communication passées et futures*

1-e Si l'on ne souhaite pas rajouter de nouveau chiffrement dans le protocole, la seule possibilité serait que STA génère une nouvelle clef de session k' à chaque exécution du protocole et l'envoie chiffrée dans le message M_3 pour assurer sa confidentialité :

M_1. $STA \rightarrow AP$: STA

M_2. $AP \rightarrow STA$: r_{AP}

M_3. $STA \rightarrow AP$: $\{r_{AP} \,||\, AP\}_k$ $_{\%}k'$ *est généré à chaque exécution du protocole*

Les sessions de communications deviennent indépendantes.

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*

$STA \rightarrow AP$: STA

$AP \rightarrow STA$: r_{AP}

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

- *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 :*

  $X/STA \rightarrow AP$: STA

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

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

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 $(M \oplus \Delta M \,||\, CRC(M \oplus \Delta M)) \oplus S$ *à partir de* $(M \,||\, CRC(M)) \oplus S$
Il suffit pour cela qu'il calcule $\Delta M \,||\, CRC(\Delta M)$*, car :*
$[(M \,||\, CRC(M)) \oplus S] \oplus (\Delta M \,||\, CRC(\Delta M)) = (M \oplus \Delta M \,||\, CRC(M) \oplus CRC(\Delta M)) \oplus S) = (M \oplus \Delta M \,||\, CRC(M \oplus \Delta M)) \oplus S$

4-b Soit $(M \,||\, CRC(M)) \oplus S$ *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 :*
$[(M \,||\, CRC(M)) \oplus S] \oplus (\Delta M \,||\, CRC(\Delta M))$

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 »).

<u>Commentaire</u> :
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, et remplace le protocole d'authentification par un protocole s'appelant le 4-way handshake. Ce dernier protocole utilise une clef d'authentification qui est spécifique à chaque exécution du protocole, et distribue une clef de session fraîche pour sécuriser les communications.