université de BORDEAUX

Master 1 *Sciences Technologies*

ANNÉE 2017-2018
Étape : Master Sciences Technologies (semestre 3)
Épreuve de : Sécurité des réseaux
Date : 19 Décembre 2017
Heure : 9h00

SESSION DE DÉCEMBRE 2017
UE : 4TIN911EX
Durée : 1h30
Documents documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer brièvement ce qu'est une clé PGP et donner quelques exemples d'utilisation de ce genre d'objets. En quoi une clé PGP est différente d'un certificat X509 ?
2. Quel est l'intérêt de l'utilisation des *One-Time-Password* ? Dans quel contexte ce genre d'objets sont-ils utilisés ? Donner un exemple d'utilisation de ce mécanisme.
3. L'une des caractéristiques du système d'authentification Kerberos est qu'un utilisateur n'a pas besoin de s'authentifier auprès du KDC chaque fois qu'il souhaite accéder à un service. Pourquoi ? Donner un avantage et un inconvénient (du point de vue de la sécurité) de cette caractéristique en les justifiant.
4. Expliquer brièvement le fonctionnement du protocole SSL/TLS. Il vous est demandé de particulièrement insister sur ce qui se passe pendant la poignée de main initiale. Qu'apporte l'utilisation des certificats par rapport à l'utilisation de clés publiques/clés privées standards ?

Exercice 1

Un utilisateur qui a pour habitude d'utiliser la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? Lire le contenu en clair des messages chiffrés reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 2

Une entreprise souhaite déchiffrer et analyser le trafic HTTPS transitant par sa passerelle. Pour ce faire, elle crée un couple certificat/clé privée correspondant à une autorité de certification (CA) et installe le certificat de cette dernière sur le poste personnel de chaque employé de telle sorte que les navigateurs internet de chaque poste fassent confiance aux certificats émis par cette CA. La passerelle quant à elle aura accès à la clé privée de l'autorité de certification.

1. Expliquer comment la passerelle peut écouter (en clair) le trafic HTTPS correspondant à une connexion établie par un navigateur se trouvant à l'intérieur de l'entreprise et se connectant à l'extérieur. Il vous est demandé de bien insister sur ce que fait la passerelle à chaque étape du protocole HTTPS.
2. Est ce que l'employé (ou plus exactement le navigateur) peut se rendre compte que sa connexion HTTPS est en train d'être écoutée ? Donner au moins une technique qui permettrait au navigateur de se rendre compte de l'écoute.
3. Dans votre réponse à la question 1 la passerelle utilise la clé privée de l'autorité de certification pour générer un certificat pour le domaine distant vers lequel la connexion est tentée (`banque.fr` par exemple). Supposons que la passerelle génère ce certificat en copiant tel quel le contenu du certificat reçu, les seuls champs à être modifiés étant le nom de la CA, la clé publique et la signature. La passerelle ne fait donc aucune vérification sur le certificat en provenance de `banque.fr` : La vérification du certificat est donc déléguée au navigateur du poste personnel. Expliquer en quoi ce scénario expose l'employé à une attaque de type *man-in-the-middle* effectuée par quelqu'un se trouvant en dehors de l'entreprise. Décrire l'attaque.

Exercice 3

L'entête des paquets IP contient un champ d'identification sur 16 bits qui est utilisé pour réassembler les fragments du paquet. Il est supposé dans IP que le champ d'identification est unique pour une paire (adresse source, adresse de destination). Une méthode classique pour implémenter un tel champ est de maintenir un compteur unique qui est incrémenté à chaque paquet envoyé. La valeur courante du compteur sera alors embarquée dans chaque paquet émis et fera office de champ d'identification.

1. Supposons qu'une machine dont le nom est Alice utilise le champ d'identification IP tel qu'implémenté précédemment. Supposons également qu'Alice réponde aux requêtes ICMP `echo-request`. Vous contrôlez une autre machine (nommons la Oscar). Comment pouvez-vous tester si Alice a envoyé un paquet à une machine autre qu'Oscar. Vous êtes autorisés à envoyer vos propres paquets à Alice depuis Oscar.
2. Votre objectif est maintenant de savoir si Bob (votre victime) exécute un service TCP qui accepte des connexions sur un numéro de port n. Vous souhaitez cacher voter identité vis-à-vis de Bob. Ainsi, Oscar ne peut pas communiquer directement avec Bob si ce n'est en usurpant l'identité d'une autre machine (i.e. forger un paquet dont l'adresse source est différente de celle d'Oscar). Expliquer comment il est possible de tester l'état du port de Bob de manière furtive depuis Oscar en utilisant Alice.

   Rappel :
   — Une machine M qui reçoit un paquet TCP contenant le flag SYN vers un port ouvert n va répondre avec un paquet contenant les flags SYN/ACK.
   — Une machine M qui reçoit un paquet TCP contenant le flag SYN vers un port fermé n va répondre avec un paquet contenant le flag RST.
   — Une machine M qui reçoit un paquet TCP contenant les flags SYN/ACK qui n'était pas attendu va répondre avec un paquet contenant le flag RST.
   — Une machine M qui reçoit un paquet TCP contenant le flag RST qui n'était pas attendu va l'ignorer.
3. Quelle modifications proposeriez-vous sur la machine Alice pour éviter ce problème ? Vous n'êtes pas autorisés à modifier le protocole TCP/IP ou les services s'exécutant sur Alice. Vous pouvez par contre modifier l'implémentation de TCP/IP sur Alice.

Problème

Lorsqu'un fichier F est téléchargé sur Dropbox depuis la machine de l'utilisateur, le client Dropbox calcule au préalable un hachage du fichier $H(F)$ et l'envoie au serveur Dropbox. Si le hachage correspond à un hachage connu du serveur (le serveur l'a déjà reçu du même utilisateur ou d'un autre), Dropbox considère que les deux fichiers sont identiques et donc ne déclenche pas le téléchargement du nouveau fichier depuis le client. Lorsque le client veut synchroniser (i.e télécharger) le fichier sur une autre machine, Dropbox va lui envoyer une copie du fichier qu'il a dans son système.

1. Supposons que la fonction de hachage H utilisée par Dropbox est telle que pour tout fichier F et malware M, il soit facile de trouver un suffixe S tel que $H(F) = H(M|S)$ où $|$ fait référence à la concaténation. Décrire comment un attaquant peut utiliser cette propriété pour propager facilement son malware M à plusieurs utilisateurs de Dropbox depuis sa propre machine. Considérer par exemple que l'attaquant a obtenu la copie d'un film très populaire avant sa sortie.
2. Quelle propriété devrait être assurée par la fonction H pour éviter le scénario de la question précédente.
3. Supposons que le tout dernier film (M) du studio `Marvel` est sur le point d'être diffusé dans les salles de cinéma. Le studio veut tester si le film a été piraté et téléchargé sur Dropbox. Expliquer comment le studio peut arriver à effectuer cette vérification en utilisant un simple client Dropbox sans avoir aucun accès privilégié aux serveurs de Dropbox.
4. La fonctionnalité de Dropbox qui a été utilisée pour répondre à la question précédente peut être utilisée pour explorer les fichiers qui sont stockés sur les serveurs Dropbox. Comment pouvez-vous modifier le fonctionnement de Dropbox pour solutionner le problème. Quelles répercutions cette solution peut-elle avoir sur la bande-passante utilisée coté serveurs Dropbox.