université BORDEAUX
Master *Sciences Technologies*

Année 2018-2019
Étape : Master Sciences Technologies (semestre 3)
Épreuve de : Sécurité des réseaux
Date : 12 Décembre 2018
Heure : 9h00

Session de Décembre 2018
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. Quelles sont les principaux apports de WPA par rapport à WEP ? Qu'en est il de WPA2 ?
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. Quelles sont les vérifications effectuées par le client (resp. le serveur) pour accepter de valider la poignée de main ?

Exercice 1

Discuter les deux scénarios suivants en terme de sécurité :

1. Deux certificats sont signés par la même clé privée.
2. Deux certificats différents ont la même signature (i.e. même résultat après chiffrement du code de hachage). À quel genre de problèmes (de sécurité) cette situation peut-elle nous confronter ?

Exercice 2

Supposons qu'un éditeur de logiciel `xyz.com` vend un produit P et veut distribuer une mise à jour de ce logiciel qu'on appellera D. L'entreprise veut assurer que ses clients n'installeront que des mise à jour publiées par l'entreprise elle-même. L'entreprise décide donc de :

— Placer D sur un de ses serveur web.
— Faire en sorte que P vérifie périodiquement si une mise à jour est disponible en utilisant `HTTPS`.

1. Que peut-il se passer si le téléchargement de D se fait au dessus de `HTTP` en lieu et place de `HTTPS`.
2. L'entreprise décide d'acquérir un un certificat pour ses serveurs web en s'adressant à une autorité de certification de confiance. Expliquer ce que P doit vérifier vis à vis du certificat du serveur pour contrer un éventuel attaquant.
3. Comment concevriez vous P ainsi que le serveur web pour que le téléchargement de D soit résistant aux attaques réseaux (actives ou passives) sans l'acquisition d'un certificat ? Vous devrez continuez à utiliser une version sécurisée d'`HTTP`.
4. Plus tard, des ingénieurs de l'entreprise ont proposé ce schéma de sécurisation :
   — Signer D avec clé privée appartenant à xyz pour obtenir une signature s.
   — Distribuer le couple (s, D) en clair à tous les clients.
   — La clé publique associée est embarquée dans P.
   Comparer l'implémentation décrite ci-dessus à l'implémentation basée sur `HTTPS` du point de vue de la puissance de calcul utilisée pour faire des calculs crytographiques. Les deux approches sont différentes lorsqu'on prend le point de vue de `xyz`. Laquelle des deux approches est la meilleure ?

Exercice 3

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 4

Sender Policy Framework (SPF) est un mécanisme simple de validation d'email utilisé pour détecter le spoofing d'emails. Le mécanisme fonctionne de la manière suivante :

— Un site tel que `gmail.cm` publie dans son enregistrement DNS une entrée SPF spécifiant l'ensemble des adresses IP pouvant envoyer des emails au nom de gmail.

— lorsqu'un serveur mail tel que `smtp.u-bordeaux.fr` reçoit un email en provenance de gmail, il vérifie que l'adresse IP du serveur source du mail apparaît bien dans l'enregistrement SPF correspondant à `gmail.com`. Dans le cas où cette adresse IP est manquante, l'email sera rejeté.

SPF est conçu (dans notre exemple) pour empêcher des machines non-gmail d'envoyer des mails en prétendant qu'ils sont issus de `gmail.com`. Pour rappel, le protocole SMTP se base sur connexion TCP sur le port 25.

1. Sans l'utilisation de SPF, n'importe quelle machine sur internet peut envoyer un email en prétendant que ce dernier est envoyé par un utilisateur gmail. À quel usage frauduleux peut servir une telle action ?

2. Supposons que `smtp.u-bordeaux.fr` choisis toujours un numéro de séquence initial nul pour l'établissement de ses connexions TCP. Expliquer comment un attaquant peut complètement contourner SPF en exploitant le fait que ce numéro de séquence initial est nul. On considérera que l'attaquant ne peut pas surveiller le réseau de `u-bordeaux.fr` (ni celui de `gmail.com`).
   Indication : Est ce que l'attaquant ne peut pas se faire passer pour une des machines de `gmail.com` ?

3. L'attaque proposée lors de la question précédente n'est pas possible si `smtp.u-bordeaux.fr` choisit un numéro de séquence initial aléatoire. Est ce que cela veut dire que SPF va empêcher toute machine ne faisant pas partie de `gmail.com` d'envoyer un mail en prétendant faire partie de `gmail.com` ? Dans cette question on considérera que l'attaquant peut surveiller le réseau `u-bordeaux.fr`.

4. Une autre défense contre le spoofing d'emails est appelée DKIM (*DomainKeys Identified Mail*) consiste à faire en sorte que gmail signe chaque email sortant. D'autre part, gmail va publier sa clé publique de vérification dans la zone DNS correspondant à `gmail.com`. Ainsi, lorsque `smtp.u-bordeaux.fr` reçoit un email prétendant provenir de gmail, le serveur va récupérer la clé publique depuis la zone DNS, vérifier la signature et n'accepter l'email que si la signature est valide. Est ce que DKIM empêche un attaquant d'envoyer des emails en se faisant passer pour un utilisateur gmail ? Expliquer.

Problème

Le professeur de sécurité informatique est toujours très paranoïaque. Il doit partir en voyage à l'étranger or il n'a pas fini de préparer l'examen final pour son cours. Il doit donc envoyer le questionnaire de l'examen, une fois terminé, à sa secrétaire pour qu'elle puisse le vérifier et l'imprimer avant le jour de l'examen final. Comme il ne veut pas prendre le risque d'envoyer le questionnaire par courrier électronique, il décide d'utiliser PGP pour chiffrer le questionnaire avant de l'envoyer. Sa clé publique est bien connue et réside déjà sur plusieurs serveurs de clés publiques. Son porte-clés (« key ring ») est déjà bien garni et contient les clés publiques de plusieurs amis, collègues et collaborateurs. Malheureusement, il remarque qu'il n'a pas la clé publique de sa secrétaire. Il lui envoie donc un courriel en lui expliquant ses intentions et la démarche à suivre :

— elle doit installer GPG,

— elle doit générer une paire de clés privée et publique,
— elle doit lui envoyer la clé publique par courriel,
— il doit chiffrer le questionnaire avec la clé publique reçue et lui envoyer le questionnaire chiffré et
— elle doit le déchiffrer avec sa nouvelle clé privée.

1. Supposons qu'une étudiante soit au courant du plan du professeur, par exemple, parce qu'elle est capable d'intercepter (« sniffer ») tout le trafic qui se dirige et/ou sort du poste de la secrétaire à partir de son portable qui est branché sur le réseau de l'école, et elle est tombée sur le courriel contenant les instructions envoyé par le professeur. Selon vous, est-ce que l'étudiante serait en mesure de se servir de tout ceci pour obtenir une copie du questionnaire avant l'examen ? Si oui comment, si non pourquoi ?

   Remarque : l'étudiante n'est pas en mesure d'empêcher le trafic de se diriger vers sa destination .

2. Le professeur, toujours très paranoïaque, ne croit pas une seconde à l'authenticité du courriel qu'il vient de recevoir de la secrétaire, contenant sa clé publique. En supposant, qu'il peut parler avec la secrétaire (par exemple, par téléphone), quel moyen peut-il utiliser pour vérifier l'authenticité non seulement du message reçu mais aussi de la clé publique reçue ? Il vous est demandé de mettre en avant deux méthodes différentes pour la vérification de la clé.

3. Supposons maintenant que le professeur est dans un endroit tellement exotique qu'il ne peut pas entrer en communication avec sa secrétaire par téléphone. Il ne dispose que d'une connexion Internet de basse vitesse (donc pas de voix sur IP ou autre mécanisme multimédia). Quel autre moyen existerait-il pour qu'il puisse obtenir une copie de la clé publique de sa secrétaire dont il soit sûr de l'authenticité ?