- After transmitting the header as a string of five characters, the interface device shall wait for a character conveying a procedure byte.

université BORDEAUX
Master 1 Sciences Technologies

Année 2016-2017
Étape : Master Sciences Technologies (semestre 3)
Épreuve de : Sécurité des réseaux
Date : 13 Décembre 2016
Heure : 11h30

Session de Décembre 2016
UE : 4TIN911EX
Durée : 1h30
Documents documents interdits
Épreuve de Monsieur Guermouche

Questions générales

1. Expliquer brièvement le fonctionnement du protocole SSL/TLS. Qu'apporte l'utilisation des certificats par rapport à l'utilisation de clés publiques/clés privées standards. Quelles sont les vérifications faites pour valider le certificat de notre interlocuteur ?
2. Expliquer brièvement les différents modes de fonctionnement d'IPSec. Il vous est tout particulièrement demandé d'insister sur ce qui est chiffré/authentifié de ce qui ne l'est pas dans chacun des cas.
3. Dans un contexte à mémoire limitée, donner deux approches pour contrer des attaques de type rejeu dans des protocoles qui y sont sensibles.
4. Donner une définition brève des attaques web de type `XSS` et `CSRF`.

Exercice 1

Soit la configuration réseau suivante dans laquelle nous voulons mettre en place un support IPSec entre les machines A et B :

Parmi les configurations IPSec suivantes, indiquer (en justifiant votre réponse) celles qui peuvent être utilisées avec de la translation d'adresse (NAT) :

1. ESP en mode tunnel.
2. ESP en mode transport.
3. AH en mode transport.

Rappel :
Lorsqu'on utilise une passerelle NAT :
— l'adresse source, et éventuellement le port source, du paquet émis est modifiée par la passerelle lorsqu'il la traverse,
— l'adresse de destination, et éventuellement le port de destination, du paquet est modifiée par la passerelle lorsque le paquet qui doit être reçu traverse la passerelle.

Exercice 2

Un pirate a remarqué qu'une requête de transfert de zone DNS (utilisée notamment pour fournir à un serveur DNS l'information qu'il doit connaître concernant la ou les zones qu'il doit desservir) fait toujours 27 octets de long, et que la réponse du serveur DNS `dns.metal.fr` fait 745 octets. On supposera que les communications se font au moyen d'UDP. De plus, le pirate dispose d'une ligne à 256 Kbps et le serveur `pauvre.victime.com` dispose d'une ligne à 5 Mbps. Enfin, le serveur `dns.metal.fr` dispose quant à lui d'une bande passante de 1 Gbps.

1. Comment le pirate peut-il réaliser une attaque par déni de service (DoS) contre le serveur `pauvre.victime.com` ? Expliquer.

Exercice 3

John Smith génère une paire de clé privée/clé publique et achète auprès d'une autorité de certification (CA) de confiance (Symantec par exemple) un certificat pour John Smith se basant sur la clé publique qu'il a générée. Il génère alors une seconde paire de clé privée/clé publique et utilise sa première clé privée (celle associée au certificat John Smith) pour signer un certificat pour lequel le nom du propriétaire (Common Name) est `www.amazon.com`. John va alors intercepter des connexions SSL/TLS vers `amazon.com`. Il va

présenter le certificat qu'il a forgé pour `www.amazon.com` aux utilisateurs dont il a intercepté le trafic. Le navigateur de l'utilisateur victime reconnaît le faux certificat comme légitime parce qu'il y a un chemin de certification valide vers une autorité de certification de confiance (Symantec).

1. En quoi ce scénario représente-t-il un danger ? Comment peut il être exploité ?
2. Comment résoudriez vous ce problème ? Ce problème est résolu en pratique. Quel mécanisme est utilisé pour détecter cela ?

Exercice 4

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

On souhaite construire un système de paiement par chèques tel que les chèques puissent être acheminés dans un réseau non sécurisé (par exemple sur Internet dans des courriers électroniques). On appelle A (pour acheteur) la personne qui émet le chèque, C (pour commerçant) la personne qui reçoit le paiement. BA est la banque de A et BC la banque de C. On construit la solution en cryptographie à clés publiques de sorte que les partenaires possède tous un couple clé publique (C) et clé privée (K). On note respectivement $(C_a, K_a), (C_{ba}, K_{ba}), (C_c, K_c), (C_{bc}, K_{bc})$ les couples de clés. Les clés publiques sont accessibles sous forme de structures de données certificats dans un annuaire de certificats. Enfin pour faire de la signature on utilise une fonction de hachage H ayant de bonnes propriétés de sécurité. La fonction de hachage sécuritaire notée H est par exemple SHA1.

Comme dans la vie courante, pour régler un achat, l'acheteur A prépare un formulaire de chèque qui comporte les coordonnées de A (l'identifiant de A qui peut comporter différentes informations dont le numéro de compte etc.), les coordonnées de C (l'identifiant du destinataire C), un identifiant unique de chèque Id_Cheq_A (un numéro de chèque de A qui doit faire qu'un formulaire de chèque a un identifiant unique) et le montant du chèque (baptisé tout simplement Montant). Toutes ces informations sont signées par A. Pour mettre le chèque en paiement, C signe le chèque en utilisant sa clé privée et transmet le chèque "endossé" à

nde APDU doit être différent de 6X et 9X ?
liées à la direction de communication de la ligne IO si cette

sa banque BC pour que le montant soit viré sur son compte. Plus formellement :

— A → C : $A, C, Id\_Cheq\_A, Montant, \{H(A, C, Id\_Cheq\_A, Montant)\}_{K_a}$
— C → BC : $A, C, BC, Id\_Cheq\_A, Montant, \{\{H(A, C, Id\_Cheq\_A, Montant)\}_{K_a}\}_{K_c}$

1. Avec ce protocole un intrus peut-il faire payer ses dépenses auprès de C en se faisant passer pour A. Comment C vérifie que seul A, a pu émettre le chèque ?
2. Avec ce protocole pourquoi la banque BC est elle sure que seul A a pu émettre le chèque, qu'il est destiné à C et que C a accepté le paiement ? Voyez vous une différence entre la signature $\{\{H(A, C, Id\_Cheq\_A, Montant)\}_{K_a}\}_{K_c}$ et l'utilisation de deux signatures concaténées : $\{H(A, C, Id\_Cheq\_A, Montant)\}_{K_a}$, $\{H(A, C, Id\_Cheq\_A, Montant)\}_{K_c}$.
3. Avec ce protocole, C peut-il présenter plusieurs fois le chèque en paiement à sa banque ? A peut-il utiliser plusieurs fois le même chèque pour payer C (le même commerçant) ou des commerçants différents ?
4. Est ce que les paiements effectués par A sont confidentiels (dans le cas où un attaquant serait capable d'écouter tout le trafic) ? Dans le cas où ca ne le serait pas, proposer une solution simple pour rendre paiements confidentiels.
5. Est ce que A peut faire des chèques sans provision ? Dans le cas où il serait possible de le faire proposer une solution simple.