PAC-1: Primera prova d'avaluació continuada

Presentació

Aquesta PAC se centra en el mòdul "Seguretat en el comerç electrònic". Hi treballarem la utilització de la criptografia com una tecnologia que permet donar seguretat a les comunicacions a través d'Internet.

Competències

- Capacitat de comunicació escrita en l'àmbit acadèmic i professional.
- Us i aplicació de les TIC en l'àmbit acadèmic i professional.
- Capacitat per analitzar un problema en el nivell d'abstracció adequat a cada situació i aplicar les habilitats i coneixements adquirits per abordar-lo i resoldre'l.
- Capacitat per proposar i avaluar diferents alternatives tecnològiques per resoldre un problema concret.

Objectius

- Comprendre les propietats bàsiques de seguretat d'una comunicació
- Conèixer la seguretat que proporciona la criptografia de clau compartida
- Conèixer la seguretat que proporciona la criptografia de clau pública

Descripció de la PAC/pràctica a realitzar

Abans de realitzar aquesta PAC és necessari haver llegit i entès els conceptes dels dos primers mòduls de l'assignatura. Es recomana cercar informació addicional a Internet.

Recursos

Bàsics

- Mòduls didàctics de l'assignatura

Complementaris

- Ordinador amb connexió a Internet i navegador web

Criteris de valoració

- Correcta redacció, amb les vostres pròpies paraules, de la resposta a cada pregunta
- Correctesa de la solució proposada a les qüestions proposades

Format i data de lliurament

La solució s'ha de lliurar en un document en format PDF abans del dia 15 d'octubre a les 23:59 hores.

Nota: Propietat intel·lectual

Sovint és inevitable, en produir una obra multimèdia, fer ús de recursos creats per terceres persones. És per tant comprensible fer-ho en el marc d'una pràctica dels estudis del Grau en Enginyeria Informàtica, sempre i això es documenti clarament i no suposi plagi en la pràctica.

Per tant, en presentar una pràctica que faci ús de recursos aliens, s'ha de presentar juntament amb ella un document en què es detallin tots ells, especificant el nom de cada recurs, el seu autor, el lloc on es va obtenir i el seu estatus legal: si l'obra està protegida pel copyright o s'acull a alguna altra llicència d'ús (Creative Commons, llicència GNU, GPL ...). L'estudiant haurà d'assegurar-se que la llicència que sigui no impedeix específicament seu ús en el marc de la pràctica. En cas de no trobar la informació corresponent haurà d'assumir que l'obra està protegida pel copyright.

Hauran, a més, adjuntar els fitxers originals quan les obres utilitzades siguin digitals, i el seu codi font si correspon.

Un altre punt a considerar és que qualsevol pràctica que faci ús de recursos protegits pel copyright no podrà en cap cas publicar-se en Mosaic, la revista del Graduat en Multimèdia a la UOC, a no ser que els propietaris dels drets intel·lectuals donin la seva autorització explícita.

Enunciat

Una empresa que es dedica a la gestió d'un aparcament privat vol implantar un sistema per gestionar-ne les reserves a través d'Internet. El procediment que se seguirà per fer una reserva és el següent:

a) Un client li envia al sistema una petició per reservar una plaça d'aparcament. En aquest missatge indica el període de temps que desitja reservar.
b) El sistema respon amb un missatge indicant-li la disponibilitat o no d'una la plaça que s'ajusti a les seves necessitats juntament amb el seu preu.
c) Si el client hi està d'acord, respon amb un missatge on indica que accepta la proposta i on comunica també el seu número de targeta de dèbit/crèdit per a que se li cobri l'import corresponent.
d) Finalment, el sistema envia un missatge al client que conté un codi que li proporcionarà accés a les instal·lacions.

El sistema ha de proporcionar les següents propietats de seguretat:

i) Ningú, a part del servidor del sistema, ha de tenir accés al número de targeta de dèbit/crèdit del client.
ii) El client no ha de poder negar el fet d'haver acceptat una proposta de plaça d'aparcament, motiu pel qual no en pot rebutjar el pagament corresponent.
iii) En el cas que hi hagués alguna incidència per accedir a la plaça de d'aparcament, el client ha de poder demostrar que disposa d'una reserva feta.

Apartat 1 (80%). Detalleu el contingut dels missatges intercanviats entre un client i el servidor del sistema així com les operacions criptogràfiques necessàries per dur a terme les següents operacions:

1) Enviament, per part del client, d'una petició de reserva.
2) Recepció, per part del sistema, d'una petició de reserva.
3) Enviament, per part del sistema, d'una oferta de plaça.
4) Recepció, per part del client, d'una oferta de plaça.
5) Enviament, per part del client, del missatge d'acceptació d'una oferta de reserva.
6) Recepció, per part del sistema, del missatge d'acceptació d'una oferta de reserva.
7) Enviament, per part del sistema, del missatge amb el codi d'accés a les instal·lacions.

8) Recepció, per part del client, del missatge amb el codi d'accés a les instal·lacions.

Apartat 2 (20%). Expliqueu, de forma detallada, de quina manera el vostre sistema satisfà cadascun dels requeriments de seguretat indicats.

Indicacions

Per motius d'eficiència computacional, cal que totes les operacions de xifratge en clau pública es realitzin utilitzant sobre digital i que totes les signatures utilitzin una funció de hash. La notació utilitzada sera:

- $AES_K(M)$: Xifrar el missatge M mitjançant el criptosistema de clau simètrica AES utilitzant la clau K.
- $AES^{-1}_K(M)$: Desxifrar el missatge M mitjançant el criptosistema de clau simètrica AES utilitzant la clau K.
- H(M): Valor hash del missatge M.
- $RSA_{Priv}(M)$: Aplicar el criptosistema de clau pública RSA al missatge M utilitzant la clau privada Priv.
- $RSA_{Pub}(M)$: Aplicar el criptosistema de clau pública RSA al missatge M utilitzant la clau pública Pub.

No us oblideu d'indicar quins participants cal que disposin d'una clau pública certificada. Recordeu que abans d'utilitzar una clau pública, cal verificar-ne la validesa. El sistema es vol que sigui lo més simple possible. En aquest sentit, la utilització d'operacions criptogràfiques que no serveixin per garantir algun dels requisits de l'enunciat es valorarà negativament.

Solució

Apartat 1

Tant el client com el servidor del sistema necessiten disposar d'una clau privada i de la corresponent clau pública degudament certificada per una autoritat en qui tothom confiï.

Enviament, per part del client, d'una petició de reserva

- El client envia un missatge indicant les dades de la reserva que vol fer.

L'enunciat no demana cap tipus de seguretat per aquest missatge. Per tant, no cal ni xifrar-lo ni signar-lo.

Recepció, per part del sistema, d'una petició de reserva

- El sistema rep el missatge, en llegeix la informació i prepara una oferta de plaça.

Enviament, per part del sistema, d'una oferta de plaça

- El sistema envia un missatge indicant les dades de la plaça ofertada al client.

L'enunciat no demana cap tipus de seguretat per aquest missatge. Per tant, no cal ni xifrar-lo ni signar-lo.

Recepció, per part del client, d'una oferta de plaça

El client rep el missatge, en llegeix la informació i estudia si la oferta s'ajusta a les seves necessitats. En cas afirmatiu, continua amb el procediment.

Enviament, per part del client, del missatge d'acceptació d'una oferta de reserva

1) El client genera un missatge, 'M', acceptant la oferta on hi consta el seu número de targeta bancària i la quantitat que accepta pagar.

2) El client calcula el resum hash de 'M', i el signa utilitzant la seva clau privada RSA. El resultat és:

$$Sig_{Client} = RSA_{ClauPrivadaClient}(H(M))$$

3) El client genera una clau aleatòria 'K' corresponent a una xifra de clau compartida, i xifra el missatge 'M', la seva signatura, i el certificat amb la seva clau pública 'Cert'. El resultat és:

$$AES_K(M, Sig_{Client}, Cert)$$

4) El client verifica la validesa del certificat del servidor comprovant-ne la signatura utilitzant la clau pública de l'autoritat de certificació. Després comprova que no ha caducat, que no ha estat revocat i finalment, comprova que les dades del propietari del certificat són correctes (en aquest cas, han de correspondre amb les del proveïdor del servei d'aparcament). Si tot és correcte, extreu la clau pública del servidor del certificat.

5) El client xifra la clau 'K' utilitzant la clau pública del servidor. El resultat és:

$$RSA_{ClauPúblicaServidor}(K)$$

6) Finalment envia els dos missatges xifrats resultants dels passos (3) i (5) al servidor.

Recepció, per part del sistema, del missatge d'acceptació d'una oferta de reserva

1) El servidor desxifra $RSA_{ClauPúblicaServidor}(K)$ utilitzant la seva clau privada obtenint la clau 'K' com a resultat:

$$K = RSA_{ClauPrivadaServidor}\ (RSA_{ClauPúblicaServidor}(K))$$

2) El servidor utiliza 'K' per desxifrar '$AES_K(M,Sig_{Client},Cert)$':

$$(M,Sig_{Client},Cert) = AES^{-1}_K(AES_K(M,Sig_{Client},Cert))$$

3) El servidor verifica la validesa del certificat del client comprovant-ne la signatura utilitzant la clau pública de l'autoritat de certificació. Després comprova que no ha caducat, que no ha estat revocat i finalment, comprova que les dades del propietari del certificat són correctes (en aquest cas, han de correspondre amb les del client amb qui s'està comunicant). Si tot és correcte, extreu la clau pública del servidor del certificat.

4) El servidor comprova la signatura digital del client mitjançant la següent comprovació:

$$H(M) = RSA_{ClauPublicaClient}\ (Sig_{Client})$$

5) El servidor procedeix a gestionar el pagament amb targeta i genera un codi d'accés per la reserva de plaça que s'està generant.

Enviament, per part del sistema, del missatge amb el codi d'accés a les instal·lacions

1) El servidor genera un missatge que conté les dades del client juntament amb el codi necessari per accedir a la reserva d'aparcament. Denotarem aquest missatge com 'N'.

2) El servidor signa aquest missatge xifrant-ne el resum hash amb la seva clau privada:

$$Sig_{Servidor} = RSA_{ClauPrivadaServidor}(H(N))$$

3) El servidor envia el missatge 'N' juntament amb la seva signatura al client.

Recepció, per part del client, del missatge amb el codi d'accés a les instal·lacions

1) El client rep el missatge 'N' i en valida la seva signatura comprovant que:

$$H(N) = RSA_{ClauPublicaServidor}\ (Sig_{Servidor})$$

Apartat 2

Requeriment 1. Ningú, a part del servidor del sistema, ha de tenir accés al número de targeta de dèbit/crèdit del client.

El número de tageta s'envia en un missatge que es xifra mitjançant un sobre digital únicament desxifrable a partir de la clau privada del servidor.

El client no ha de poder negar el fet d'haver acceptat una proposta de plaça d'aparcament, motiu pel qual no pot rebutjar el pagament corresponent.

El client indica la seva conformitat mitjançant un missatge que s'envia signat digitalment. Per tant, aquest missatge és no repudiable.

En el cas que hi hagués alguna incidència per accedir a la plaça de d'aparcament, el client ha de poder demostrar que disposa d'una reserva feta.

Un cop la reserva ha estat acceptada, el servidor envia un missatge signat al client amb tots els detalls de la reserva. En cas d'incidència, el client el pot mostrar. La signatura digital en demostra la seva autenticitat.