Aplicacions i Serveis a Internet

durada 3h

Final - Juny 2019

1. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat.

   a) És possible servir més d'una web en una xarxa privada i que es pugui accedir a elles amb diferents noms de domini només obrint únicament el port 80 de l'encaminador NAT que és l'únic que té l'adreça pública.

   b) Un certificat d'usuari només és confiable si l'he rebut d'algú amb qui confio i per un canal confiable.

   c) Servir un fitxer a algú a través de la URL https://servidor/xhjasldkdji/fitxer.dat on aquesta URL s'envia per un canal confidencial a aquest algú, és un mecanisme que garanteix la confidencialitat.

   d) Si la clau pública només es rep de persones de confiança, deixen de tenir sentit les autoritats certificadores.

   e) Si una persona genera el parell de claus públic i privat, pot xifrar missatges per a ella mateixa i signar missatges per tothom.

   f) Si un client vol autentificar-se amb un servidor generant un parell de claus pública i privada, li ha de proporcionar al servidor la clau pública de manera que cada vegada que es connecti, el servidor pugui comprovar que és ell. En canvi el servidor no cal que generi cap parell de claus.

   g) Un certificat digital és el resultat de xifrar el valor de la clau pública d'una identitat, fent servir la clau privada d'una altra entitat de la que coneixes de manera fiable el valor de la seva clau pública.

   h) Un missatge signat no és fiable si s'ha rebut per un canal que podem assegurar que no és fiable.

   i) L'obtenció d'un certificat d'usuari implica que l'autoritat de certificació podria desxifrar els missatges d'aquest usuari.

   j) Quan unes claus caduquen, els documents signats amb aquestes claus també caduquen.

   k) El mecanisme de Sockets permet el pas de missatges entre processos de diferents màquines però no entre processos de la pròpia màquina.

   l) Quan es compra un domini, el gestor al que li contractes demana al responsable del top level domain una entrada a la seva base de dades amb un registre NS del domini registrat cap a un servidor de DNS autoritatiu gestionat pel propi gestor.

   m) Si algú accedeix a la nostra clau privada, el que s'ha de fer és canviar la contrasenya de la clau immediatament per continuar garantint la seguretat.

   n) El mecanisme per garantir la restricció d'accés a certes pàgines dins d'una mateixa web s'aconsegueix a través de les cookies.

   o) Quan acceptem les cookies d'un lloc web, aquest lloc podria accedir a la informació personal que tenim al nostre ordinador.

   p) Si accedim al nostre banc a través d'una xarxa insegura, no podem fer res per assegurar les nostres comunicacions.

   q) Es pot simular l'enviament de dades d'un formulari amb un navegador web sense accedir al formulari si el mètode del formulari és GET.

   r) Fent servir un navegador web, si el mètode d'un formulari és POST, no existeix cap altre manera per enviar les dades que primer accedint al formulari i després polsar el botó enviar. És a dir, no es poden enviar les dades amb una única petició.

   s) Un smarthost que accepta ser-ho per qualsevol adreça IP és un servidor potencial de correu spam.

   t) El remitent d'un correu electrònic sempre ha de ser una adreça de la qual existeixi una bústia en algun servidor amb aquest mateix nom.

2. La generació de correu "spam" consisteix en l'enviament de missatges de correu no desitjats a les bústies de diferents destinataris. Respon sí o no i justifica si les següents estratègies serveixen per evitar la generació de correu "spam".

   a) Un smarthost autentifica amb usuari i contrasenya la connexió SMTP que li lliura missatges per enviar

   b) El servidor que accepta certs dominis analitza que la màquina client que se li connecta tingui un servidor de correu funcionant

   c) El servidor que accepta certs dominis analitza que la màquina client que se li connecta tingui la IP corresponent al domini amb el que es presenta quan estableix la connexió SMTP

   d) El servidor que accepta certs dominis analitza que la màquina client que se li connecta tingui com resolució inversa el domini amb el que es presenta en funció de la IP de connexió

   e) El servidor que accepta certs dominis analitza si el domini que es dóna amb la comanda MAIL FROM existeix al DNS

3. Respon sí o no i justifica si els següents mecanismes serveixen per autentificar múltiples vegades (evitar atac de grabació) a un usuari A davant d'un usuari B. Considereu que si no es diu el contrari, la comunicació no està xifrada. Quan es parla de contrasenya, tant A com B la coneixen.

   a) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge H(m) com a prova de la seva identitat, on H(m) és el resultat d'aplicar una funció de hash coneguda.

   b) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge aleatori generat per A i m1|m2 és la concatenació dels dos missatges. H() és una funció de hash coneguda.

   c) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge K(m) que és el resultat d'aplicar una transformació a m on aquesta funció K() de transformació només és coneguda per A i B.

   d) Usuari B envia un missatge aleatori m a A. A retorna a B el missatge H(m1|m2) on m2 és un missatge fixe conegut només per A i per B. H() és una funció de hash coneguda.

   e) Usuari B espera la recepció d'un missatge c de A, on c és un la contrasenya associada a A.

   f) Usuari B espera la recepció d'un missatge m de A, on m = KBp(c) és la contrasenya associada a A xifrada amb la clau pública de B.

   g) Usuari B espera la recepció d'un missatge m de A, on m = K(c) és la contrasenya associada a A xifrada amb una clau només coneguda per A i B.

   h) Usuari B envia un missatge aleatori m1 a A. A retorna a B el missatge KBp(m2) on m2 és un missatge aleatori generat per A. La concatenació K = m1|m2 és la clau de sessió d'un algoritme conegut de xifrat simètric. Usuari A envia K(c) a B, on c és la contrasenya associada a A i coneguda per B.

4. Considereu el següent algoritme:

   - Es busca dos nombres primers p, g on $p>g$. Aquests nombres s'intercanvien entre l'interlocutor I_A i el I_B.
   - L'interlocutor I_A genera un nombre aleatori $a<p$ i calcula $A = g^a mod p$ que envia a I_B.
   - L'interlocutor I_B genera un nombre aleatori $b<p$ i calcula $B = g^b mod p$ que envia a I_A.
   - a i b són només coneguts per I_A i I_B respectivament.
   - $I_A$calcula $K_A = B^a mod p$ i $I_B$calcula $K_B = A^b mod p$

   a) Demostreu que $K = K_A = K_B$

   b) Justifiqueu el perquè algú que observi l'intercanvi de missatges no pot aconseguir el valor de K

   c) Calculeu el valor que surt de K tant per l'interlocutor I_A com $I_B$considerant els següents valors p=23, g=5, a=6, b=7.