Aplicacions i Serveis a Internet

durada 3h

Final - Juny 2018

1. Preguntes cert o fals. Justifiqueu la resposta. Les respostes incorrectes resten. Les respostes sense justificació compten la meitat. (5)

   a) És possible tenir més d'un servidor web en una xarxa privada i que es pugui accedir a ells 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 l'únic que fa es demanar 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 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 a internet 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. Respon sí o no i justifica si els següents mecanismes serveixen per autentificar a un usuari A davant d'un usuari B tantes vegades com calgui. Considereu que si no es diu el contrari, la comunicació no està xifrada. Quan es parla de contrasenya, tant A com B la coneixen: (2)

   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.

3. Per aconseguir les credencials d'un usuari es fa el següent muntatge. Complementeu i/o justifiqueu la viabilitat d'aquest atac. Responeu amb un sí o un no: (0.5)

   - Es munta un punt d'accés WIFI que oferix accés a Internet.
   - Es munta un servidor de DHCP i de DNS local on els registres de DNS que ofereix estan manipulats per oferir les adreces IP que desitgi l'atacant.
   - Es munta un servidor web amb una semblança idèntica al servidor del que es volen conèixer les credencials.
   - Aquest servidor disposa de la capa TLS i per tant fa servir el protocol https.
   - Quan l'usuari vol connectar al servidor web, el servidor de DNS local li dona la IP on el troba el servidor web falsificat.
   - Considereu que l'usuari disposa d'un navegador web estàndard sense cap tipus de manipulació.

4. Descriviu tot el procés previ a establir la connexió amb un servidor web per aconseguir la seva adreça IP a partir del seu nom de domini. (0.5)

5. Un TIC espavilat decideix muntar un servei consistent en oferir la capa TLS a qualsevol web existent que no tingui aquesta capa de seguretat. Per fer-ho, sol·licita als seus clients que el servidor d'autoritat del domini dels clients sigui el seu servidor DNS. Un cop fet això, fa que tots els dominis dels seus clients resolguin a la única adreça IP 83.5.5.5 on té un servidor web. Els clients han de disposar de la seva pròpia web http, ja sigui a internet o a dins de la seva xarxa privada. En aquest últim cas aquesta web ha de ser accessible des de internet. (1)

   a) Descriu qualitativament com s'ha de fer aquest muntatge (serveis i configuracions).

   b) Si una empresa té més d'una web, servides per diferents servidors a la seva xarxa privada i totes elles només accessibles internament, es poden servir a través del port 80 aprofitant el servei d'aquest TIC espavilat? En cas que calgui afegir alguna cosa a l'empresa, busque-ho l'alternativa més simple.

6. Un mecanisme per obtenir un certificat vàlid d'una autoritat certificadora per un servidor web amb nom empresa.cat consisteix en el següent: L'autoritat certificadora disposa d'una web http://web-autoritat on es rep la petició del certificat. L'autoritat genera un correu al destí certificat@empresa.cat amb una URL única del tipus (https://web-autoritat/seq-aleatòria-associada-empresa-cat). Aquesta URL es l'enllaç de descàrrega del certificat. (1)

   a) Consideres que és un mecanisme vàlid per concedir el certificat? Justifica.

   b) En què consisteix la petició del certificat que es fa a la http://web-autoritat?