Pràctica SSL/TLS Certificats digitals

Curs 2019 - 2020

Al web de l'assignatura ASIX-M11 trobareu a la UF2 els materials corresponents a aquesta activitat "Certificats digitals, TLS/SSL". Hi ha varis dossiers molt extensos:

objectius TLS/SSL

Descripció dels objectius a aprendre.

HowTo-ASIX_Certificats_Digitals

Manual / Apunts a seguir, explica com crear certificats i com utilitzar-los per a comunicacions client/servidor amb SSL/TLS

Howto-ASIX-Examinar_SSL.pdf

Examinar tràfic TLS/SSL. Us descriu uns quants exemples amb eines per investigar el tràfic SSL. Us serà útil per entendre què passa quan connectem per exemple per https o ldaps.

També us serà útil per fer test i verificar el funcionament dels vostres certificats en comunicacions segures ldap i opnvpn.

ECHO Server / ECHO Client

Un exemple de SSL Python. Els programes echo client i echo server que vam fer a M06 UF2 converrtits a SSL/TLS per poder-los utilitzar en una comunicació segura.

Annexos

Extra: doc_m08_ioc_correu_annexos (Annex global dels apunts IOC de correu)

Consultar només les parts:

- extracte Annex A2: Seguretat conceptes generals
- extracte Annex A5: OpenSSL Certificats digitals

En aquests dossiers trobareu uns extensos rotllos explicatius de què son i com funcionen els certificats…. LLEGIU-HO!

Pràctica a realitzar:

Aquest tema s'avalua en dues pràctiques que es fan a l'aula in situ però que l'alumne prepara a casa, desplega a l'aula i li ensenya al professor, tot explicant què fa i contestant les preguntes que rep.
Excepcionalment caldrà que elaboreu un document en markdown explicant el procés, amb incrustacions tant del codi per generar els certificats, la imatge i els serveis segurs, com de l'explotació dels serveis segurs. Ha de ser palpable que el tràfic és segur.

1) Servidor ldap segur

   Crear una nova imatge docker del servidor ldap que implementi un servidor ldap segur. Ha d'utilitzar els seus propis certificats digitals i ha de permetre tant connexions ldaps com connexions ldap amb starttls.

   Utilitzarem sempre una autoritat de certificació CA anomenada Veritat Absoluta, que és qui emetrà tots els certificats per a l'organització edt.org. Aquí caldrà un certificat de servidor ldap.edt.org (si pode posar-li àlies millor).

   Un client ldap ha de poser-se conectar al servidor ldap usant ldaps connectant al port privilegiat, però també usant ldap (port insegur) i usant startls per generar una connexió segura.

   Assegureu-vos de practicar amb telnet, curl, i ldapserach (amb zetes!) fins a tenir-ho clar.

2) OpenVPN amb certificats propis.

   Implementar els exemples de OpenVPN (3,4) però utilitzant certificats pròpis i no els certificats per defecte de OpenVPN. I l'exemple amb systemctl i un servidor a AWS EC2 i dos clients locals

   Utilitzarem sempre una autoritat de certificació CA anomenada Veritat Absoluta, que és qui emetrà tots els certificats per a l'organització edt.org. Aquí caldrà un certificat de servidor i un parell de certificats client. Atenció que segurament els certificats han de complir uns requeriments específics per a ser vàlids per a OpenVPN.

   Recordeu també de posar atenció el nom del certificat (mireu de posar-hi àlies).

Repàs general de conceptes

En treballar amb GPG ja hem ist els conceptes de criptografia simètrica i asimàtrica, clau privada i clau pública i de certificat. També el de web of trust i de PKI Public Key Infrestructure. I sabem el significat de xifrar, signar, autenticar i no repudi.

Un cosa són els certificats digitals i l'altra les comunicacions segures. Les comunicacions segures SSL/TLS necessiten dels certificats digitals per funcionar. Els certificats digitals es poden fer servir en altres àmbits.

Certificats digitals

Permeten identificar una persona, entitat, servidor, etc. El dni, el certificat de una web, el certificat de notes, etc.

Utilitzen criptografia asimètrica, consten d'una clau privada (a mantenir secreta) i una pública (a publicitar com més millor). Però això no són certificats, són parelles de claus priv/pub.

Un certificat digital és la suma de: una clau pública + les dades del subject + el segell o firma de una autoritat. Igual que un certificat de notes de l'alumne són les dades de l'alumne, el seu dni que l'identifica més el segell de l'escola que autentica que són certes.

Per tant per tenir un certificat digital cal una CA que 'firmi' avali el certificat. Pot ser un organisme públic (la generalitat), un de privat (letsencrypt) o un de propi (la propia organització o empresa es constitueix en CA). Probablement té més credibilitat la Generalitat de Catalunya que la nostra organització Veritat Absoluta (inventada) però si fem funcionar tota l'organització edt.prg sota aquesta CA els certificats seran vàlids dins de l0organització.

Un bitllet de 500€ signat pel banc d'espanya té més credibilitat que signat per mi. Però un paper signat per mí dient 10€ de regal al meu fill té tota la validesa per a ell.

Crearem una CA Veritat Absoluta per a signar altres certificats.

Quan un usuari o un servei vol demostrar qui és el que fa és obtenir un certificat digital. Per exemple el servei web http.edt.org vol un certificat per permetre conexions segures https.

Li cal primer generar una parella de claus privada/pública. Llavors generar una petició de certificat, que és la combinació de la clau pública més les dades de l'usuari (el CN, O, L, CT… els camps que el descriuen en format de Distinguished Name que ja n¡coneixem de ldap).

La petició de certificació s'envia a l'entitat CA que ha de generar el certificat (issuer), que el signa amb la seva clau provida estampant-li el seu segell. Observeu que un certificat no és més que la clau pública del subjecte, les seves dades personals i la firma de la CA.

Observeu que en firmar la CA amb la seva clau privada la resta del món pot comprovar que el certificat és vàlid a través de la clau pública de la CA.

****nota** Aquí us recomano que invertiu de 2h a 4h jugant amb la bogeria de ordres ssl fins que sapigueu examinar del dret i del revés que és una clau privada, una clau pública, un request i un certificat. Això és el que fariem a classe fins a sagnar els dits! Ens sabriem de memòria què fa cada una de les opcions de openssl com per exemple openssl x509 -text --noout -in server-cert.pem.**

nota tot i que en molts exemples posen extensions .cert i .key NO HO FEU. L'extensió és sempre .pem, poseu al nom del fitxer si és un cert, una key o un request, per exemple server.cert.pem o server-key.pem.

Tip:
Podeu generar certificats autosignats, és el més ràpid però no us serviran en les pràctiques perquè generalment es descarten, no es consideren prou segurs. De manera que us aconsello que genereu sempre certificats signats per una CA.

Servei Segur https: SSL/TLS

L'exemple més típic és implementar un servei segur https. Quan parlem de comunicacions de xarxa segures, de tràfic segur i posem la s al final hhtps, ldaps, etc és que estem utilitzant SSL/TLS.

Per poder utilitzar SSL/TLS cal que almenys el servidor disposi del certificat digital que l'authentica. Observeu que també es pot requerir que el client tingui el seu certificat digital (per exemple per autenticar-te com a client amb hisenda, amb la generalitat, etc).

En aquest punt heu de fer la pràctica de muntar un servidor http amb certyificat digital propi (està als apunts). Cal observar els següents casos:

- Si el servidor web té un certificat autosignat el primer cop que el navegador client connecta a la web es genera una excepció. Si s'accepta l'excepció (incorpora el certificat del servidor) les següents connexions ja no es generarà l'excepció.

- Si el servidor té un certificat provinent de la CA veritat Absoluta i el navegador no té aquesta entitat entre les entitats Trusted, es generarà la excepció…

- Si el servidor té un certificat digital signat per la CA veritat Absoluta i en el navegador hem carregat (abans!) el certificat de la CA, en connectar a la pàgina web ja no es generarà cap excepció (perquè rep un certificat d'una entitat trusted).

Proveu això del dret i del revés, examineu els certificats carregats al navegador de servidors i d'entitats. Atenció, el caché del navegador us farà la pirula, **no us deixeu enganyar, al loro!**.

PROBLEMA: Fer certificats digitals i serveis segurs és ben fàcil però es perden moooooltes hores per culpa d'una estupidesa, el certificat és a nom per exemple de http.edt.org i les proves les faig connectant a localhost o a 172.17.0.2. Si el nom del destí amb el que conecto no és ***exactament*** el mateix que el del certificat no funcionarà.
És a dir, NO fem conexions a localhost a a la ip si el certificat està emès a un altre nom de subject

AVANÇAT: es poden fer certificats per a conjutns de hosts, tipus *.edt.org o *.localdomain i es poden fer servir alternative names. A part del nom definit en el subject es pot afegir una extensió amb varis noms alternatius per al certificat, que serà vàlid per a tots aquests noms.

SSL/TLS i STARTLS

Si hem sabut fer un servidor web amb https també hem de saber fer un servidor ldap amb ldaps, simplement cal generar el certificat apropiat, per exemple de ldap.edt.org. Siho fem així podem connectar amb ldaps al servidor ldap:
Per exemple: ldapsearch -x -H ldapd://ldap.edt.org -b 'dc=edt,dc=org' dn

Però també podem configurar el servidor ldap (i el de altres serveis) per permetre connexions segures no al port segur sinó al port insegur. Són connexions que comencen amb text pla però que amb STARTTLS es converteixen en comunicacions segures.

Aquí us cal implementar un servidor ldap segur que permeti connexions segures ldaps i ldap+STARTTLS.

Estructura PKI i Automatització

En els apunts veureu com podeu esdevenir una CA i automatitzar el procés d'emissió de certificats amb una estructura de directoris que es crea automàticament a /etc/pki. Si es configuren apropiadament els fitxers de configuració podreu anar emetent certificats amb uns valors per defecte (que podeu redefinir o modificar per a casos concrets). Veureu que a cada certificat s'incrementa el serial number de certificat emès.

aquesta part és un pèl més complicada

Confiuració de certificats i extensions

La part final dels apunts fa un repàs al fitxer de configuració de openssl. N'hi ha un de general si estem treballant en mode infraestructura (el de /etc/pki…) però en podem fabricar de adhoc per usar en una determinada ordre.

Si enteneu l'estructura del fitxer veureu que hi té seccions on es defineixen valors (els valors predefinits), però es poden definir altres seccions, per exemple una per a definir valors per a certificats de profes, i una secció diferent per a definir valors per a certificats d'alumnes. En cridar l'ordre openssl li podem indicar quines seccions volem usar.

Un dels elements més importants del fitxer de configuració és la definició d'extensions, que permeten ampliar i restringir la funcionalitat del certificat, per a que serveix i per a què no. Podem fer un certificat que serveixi per autenticar el correu però no per autenticar un servidor, que serveixi per encriptar però no per autenticar…

En aquest punt ens cal batallar per a poder fer certificats de OpenVPN vàlids per al servidor i per als dos clients, tots tres signats per la CA Veritat Absoluta. Aquests certificats de OpenVPN han de complir determinats requisits.