Taller de Administración de Servidores Linux

CC5308

Clase 19: 21 de Abril de 2011

Certificados Digitales (HTTPS)

Eduardo Mercader Orta
emercade [at] nic . cl

Introducción

- Justificación de la necesidad de HTTPS
- Certificado digital
- Cadenas de confianza
- Autoridad certificadora
- openssl
- Listas de revocación
- Validaciones
- Solicitudes de firma de certificados
- Certificados autofirmados para sitios WEB
- Futuro ... ¿ DNSSEC ?

Certificado digital

- Certificado de llave pública, la parte privada de la llave la conoce solo el propietario.
- Permite identificar al propietario, por medio de la firma de una entidad de confianza.
- Contiene identidad titular, clave pública, identidad de quien firma el certificado, algoritmo de firma, fecha de inicio y de expiración, número de serie.
- Usualmente en formato X.509
- Se usan para autenticación y cifrado de conexiones

Cadenas de confianza

- Mecanismo de generación de confianza
- Generadas a partir de información previa en los Browser
- WebTrust, http://www.webtrust.org/
- CA/Browse forum, http://www.cabforum.org/
  - Apple, Google, KDE, Microsoft, Mozilla, Opera, RIM
  - Muchas autoridades certificadoras
  - Acuerdo para la definición y uso de certificados EV (Extended Validation).
- ca-bundle

Autoridad Certificadora

- Mercado concentrado Verisign (47.5%), GoDaddy (23,4%), Comodo (15,44%), de acuerdo a Netcraft SSL Survey 2009
- En Chile Ministerio de Economía regula el mercado ver, http://www.entidadacreditadora.cl
- CAcert.org, autoridad certificadora de la comunidad que entrega certificados gratuitos
- OpenCA, software para crear autoridades certificadoras (openldap+openssl+apache, entre otros)
- Grandes barreras de entrada a pesar de openssl

openssl

- Comando básico para operaciones con certificados en Unix/Linux y derivados
- Es una caja de herramientas que permiten la manipulación del SSL (Secure Socket Layer v2 y v3), del TLS (Transport Layer Security v1) network protocol y de estandares criptográficos asociados
- Es un comando para terminal que permite:
  - Creación y administración de llaves y parámetros
  - Operaciones sobre llaves criptográficas públicas
  - Creación de certificados X509, CSRs y CRLs
  - Cálculos de reducciones (digest) y test de clientes y servidores y otros (como mensajes S/Mime)

Listas de revocación

- CRL (Certificate Revocation List)
- Permite identificar los certificados que han sido revocados (comprometidos y/o anulados)s
- La lista permite indicar dos estados:
  - Revocado (Revoked), anulado en forma irrevocable, usualmente debido al compromiso de su llave privada o a una emisión errónea.
  - Suspendido (Hold), suspendido temporalmente, mientras el titular verifica la pérdida de la llave privada o su compromiso.
- Problema, su distribución.
- OCSP (Online Certificate Status Protocol)

Validaciones

- Los certificados deben validarse con respecto a:
  - Fecha de inicio de su validez (“no antes de”)
  - Fecha de fin de su validez (“no despues de”)
  - Firmas de la cadena de confianza hacia la autoridad certificadora
  - Fecha de inicio y de final de la validez de certificados en la cadena de confianza
  - Listas de revocación de la autoridad certificadora o mecanismos tipo OCSP. Esto puede conllevar problemas de denegación de servicios.

Requerimiento de firma de certificados

- CSR (Certificate Signing Request)
- Usualmente basado en la especificación PKCS#10 RFC 2986
- El titular crea un par de llaves (pública y privada)
- El CSR generado contiene la llave pública y la información de identidad del titular
- El CSR debe ser enviado a la autoridad certificadora, si lo acepta, devolverá un certificado digital firmado que contendrá la información de identidad, la llave pública y demás información.
- La llave privada no se debe incluir en el CSR

Certificados autofirmados para sitios WEB

- Permiten activar sitios Web con protocolo HTTPS
- Requieren confianza en el certificado autofirmado por parte del usuario que se autentica
- Requieren generar para de llaves y CSR
- Se utiliza openssl para generar llaves, CSR y certificado
- Instalación de llave privada en el servidor

FUTURO

¿ DNSSEC ?

Actividad Personal

Usando openssl procedo a:

- Genero llave privada
- Creo CSR
- Genero certificado autofirmado

Configuro un sitio virtual con apache que use https como protocolo base y pruebo la conexión (requiere mod_ssl instalado)

SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/www.midominio.cl.crt
SSLCertificateKeyFile /etc/pki/tls/private/www.midominio.cl.key

Actividad Personal

Comandos

```
# openssl genrsa -out www.midominio.cl.key 2048
# openssl req -new -key www.midominio.cl.key  -out www.midominio.cl.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CL
State or Province Name (full name) []:Santiago
Locality Name (eg, city) [Default City]:Santiago
Organization Name (eg, company) [Default Company Ltd]:Mi empresa
Organizational Unit Name (eg, section) []:Ingenieria
Common Name (eg, your name or your server's hostname) []:www.midominio.cl
Email Address []:admin@midominio.cl

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
# openssl x509 -req -days 365 -in www.midominio.cl.csr -signkey www.midominio.cl.key -out www.midominio.cl.crt
key www.midominio.cl.key -out www.midominio.cl.crt
Signature ok
subject=/C=CL/ST=Santiago/L=Santiago/O=Mi empresa/OU=Ingenieria/CN=www.midominio.cl/emailAddress=admin@midominio.cl
Getting Private key
# ls
www.midominio.cl.crt  www.midominio.cl.csr  www.midominio.cl.key
# openssl x509 -in www.midominio.cl.crt -text
```