Les concepts de protocoles et d'algorithmes cryptographiques

Cryptologie, résoudre des problèmes de sécurité associés à la communication en réseau via des protocoles cryptographiques:

- L'échange confidentiel d'informations
- L'authentification des participants

Ces protocoles cryptographiques utilisent des algorithmes cryptographiques:

- de chiffrement
- De générateurs d'empreintes (fonctions de hachage)

Les concepts de protocoles et d'algorithmes cryptographiques

Quelques protocoles:

- PGP: protocole pour chiffrer et signer des e-mails
- S/MIME: protocole pour chiffre et signer des e-mails basé sur une PKI x509
- Kerberos: protocole assurant l'authentification et la confidentialité
- SSH: protocole assurant l'authentification et la confidentialité
- SSL: idem que SSH, basé sur un PKI 509
- IPSEC: Protocole VPN

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement

C’est algorithmes ont pour rôle de rendre incompréhensible un message à toute autre personne que son destinataire.

Les algorithmes de chiffrement sont de deux types:

- Symétriques: à clé secrète
- Asymétriques: à clé publique

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement symétrique

Un message en clair est chiffré (crypté) en utilisant une méthode cryptographique avant d'être transmis au correspondant.

Exemple: la méthode de Jules César, décalage de N lettres

Pour un décalage de 3 lettres BONJOUR devient …….

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement symétrique

Les algorithmes à clé secrète:

- DES
- 3DES
- AES
- RC4
- …

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement symétrique

TP:

gpg --symmetric fichier

gpg --decrypt fichier.gpg

openssl aes-256-cbc -in fichierEnClair -out fichierCrypter

openssl aes-256-cbc -in fichierCrypter -out fichierEnClair

vim -x fichier

file fichier

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement asymétrique ou à clé publique

L’algorithme à clé publique utilise deux clés, une clé publique et une clé privée.

Ces deux clés sont générées ensemble et elles dépendent l’une à l’autre.

La clé publique peut être publiée sans risque, mais la clé privée doit être conservée secrète par son propriétaire.

La clé publique sert habituellement à crypter un message et la clé privée à la décrypter, mais l’inverse est possible.

Les concepts de protocoles et d'algorithmes cryptographiques

Les algorithmes de chiffrement asymétrique ou à clé publique

TP:

- User1 génère un couple de clés

openssl genrsa -out cle.pem 1024

- User1 extrait la clé publique

openssl rsa -in cle.pem -pubout -out pub.pem

- User2 chiffre le fichier en utilisant la clé publique de User1

openssl rsautl -inkey pub.pem -pubin -in fichier.txt -out fichier.crypt -encrypt

- User1 déchiffre avec sa clé privée

openssl rsautl -inkey cle.pem -in fichier.crypt -out fichier.txt -decrypt

Les concepts de protocoles et d'algorithmes cryptographiques

Les fonctions de hachage

Elles permettent de créer l'empreinte numérique d'un message. Si l'on modifie le message, l'empreinte associée est complètement différente.

Les fonctions de hachage vérifient qu'un message ou un fichier n'a pas été altéré.

Les concepts de protocoles et d'algorithmes cryptographiques

Les fonctions de hachage

TP

- sum fichier
- md5sum fichier
- sha1sum, sha256sum, sha512sum fichier
- openssl dgst -(md5 ou sha1 ou sha256 ou sha512) fichier

La signature numérique, les certificats X-509, la notion de PKI

La signature numérique

La signature numérique, comme une signature manuscrite, a pour objectif d'identifier l'auteur d'un document et d'en prévenir toutes falsification.

La signature numérique

TP

User1

openssl dgst -md5 fichier.txt > fichier.md5

openssl rsautl -sign -in fichier.md5 -inkey cle.pem -out fichier.sig

User2 reçoit le fichier et la signature:

openssl dgst -md5 fichier.txt

openssl rsautl -verify -in fichier.sig -inkey pub.pem -pubin

La signature numérique, les certificats X-509, la notion de PKI

Les certificats X-509

Un certificat numérique est un document qui comprend essentiellement une clé publique et des renseignements sur le propriétaire de cette clé, le tout signé avec la clé privée d'un organisme reconnu, un CA (Certification Authority).

X509 permet l'authentification en réseau.

La signature numérique, les certificats X-509, la notion de PKI

Les certificats X-509

TP:

- **Génération d'un certificat auto-signé**

openssl req -x509 -nodes -newkey rsa:2048 -keyout test.key -out test.crt -days 365

openssl x509 -in test.crt -text -noout

- **Génération d'un certificat auto-signé avec l'option subj**

openssl req -x509 -nodes -newkey rsa:2048 -keyout test.key -out test.crt -days 365 \

-subj "/C=SN/ST=Senegal/O=Test/CN=server.test.sn"

La signature numérique, les certificats X-509, la notion de PKI

Les certificats X-509

TP: Requête de signature pour un certificat valide

- Créer un couple de clés publique/privée

openssl genrsa -out cle.key 2048

NB: la clé publique est contenue dans la clé privée:

openssl rsa -in cle.key -pubout

- **Créer une requête de certificat**

openssl req -new -key cle.key -out cle.csr

La signature numérique, les certificats X-509, la notion de PKI

Les certificats X-509

TP: Requête de signature pour un certificat valide

Le fichier cle.crt doit être à l'autorité de certification pour signature.

Exemple: https://order.digicert.com/step1/ssl_basic?validity=3

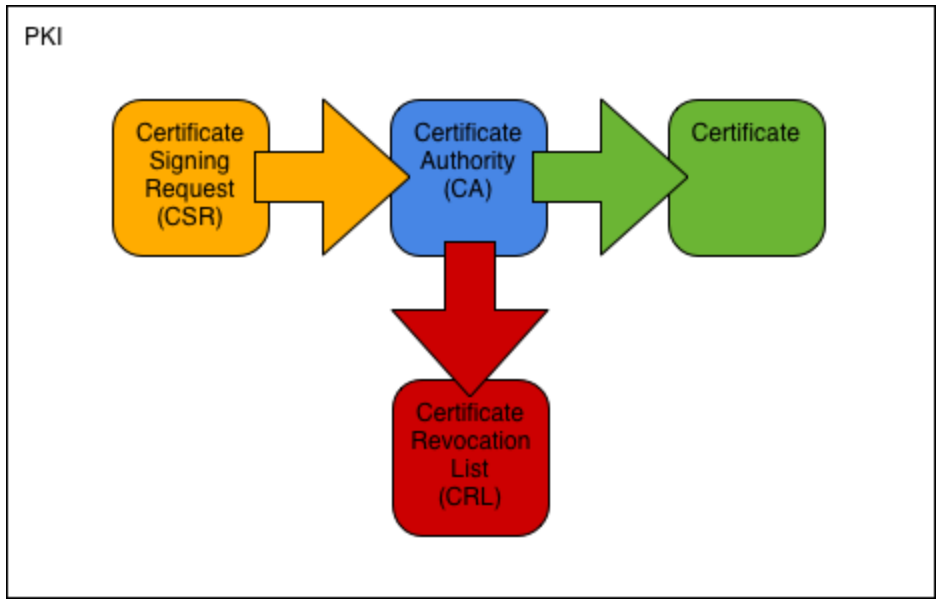
La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

Une PKI (Public Key Infrastructure) est une organisation centralisée, gérant les certificats x509 afin d'instaurer la confiance dans les échanges de données, principalement en permettant l'échange de clés publiques et l'identification des ordinateurs et des individus.

Composants d'une PKI:

- Les certificats
- Les CAs
- Les CRLs



La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

1) Les certificats

Un certificat associe une clé publique et des données d'identités, le tout signé par un CA.

L'identité d'un utilisateur est généralement son adresse e-mail. L'identité d'un serveur est son adresse DNS complète (FQDN).

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

2) Les CAs

Le CA (Certification Authority)

- Il crée les certificats (en les signant).
- Il doit vérifier l'authenticité des données présentes dans une requête de certificat.

Ainsi il les garantit via sa signature.

Il existe deux types de CA

- Les CA public : leurs certificats vérifient l'identité des serveurs sur Internet.
- Les CA privés : c'est un CA interne à une société. Ils permettent de créer une PKI interne

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

3) Les CRL (Certificate Revocation List)

Si **un pirate obtient la clé privée** d'un serveur, il peut écouter toutes les transactions de celui-ci.

Dès que la compromission a été détectée, il faut créer un **nouveau certificat et révoquer l'ancien**.

Une CRL contient, au niveau d'un CA, la liste des certificats révoqués qui n'ont pas encore expiré.

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

1. Création de l'arborescence: avec le compte d'un utilisateur simple

```
mkdir ~/SSL/
cd ~/SSL
mkdir private
mkdir cacerts
mkdir demoCA
mkdir newcerts
touch demoCA/index.txt
echo "01" > demoCA/serial
```

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

2. Génération d'un certificat auto-signé pour le CA

```
openssl req -x509 -days 3650 -newkey rsa:2048 \
-keyout private/caKey.pem \
-out cacerts/caCert.pem
```

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

3. Génération d'une requête de signature de certificat pour le serveur Apache et signature de la requête par le CA

```
openssl req -nodes -newkey rsa:2048 -keyout private/serverKey.key \
-subj "/C=SN/ST=Senegal/L=Dakar/O=Test/CN=server.test.sn" -out private/serverReq.csr

openssl ca -in private/serverReq.csr -days 365 -cert cacerts/caCert.pem -keyfile private/caKey.pem \
 -outdir newcerts/ -out newcerts/serverCert.crt
```

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

4. Génération d'une requête de signature de certificat pour le client et signature de la requête par le CA

```
openssl req -newkey rsa:2048 -subj "/C=SN/ST=Senegal/O=Test/CN=diokh"  \
-keyout private/diokhKey.key  -out private/diokhReq.csr

openssl ca -in private/diokhReq.csr -days 365 -out newcerts/diokhCert.crt -notext \
-cert cacerts/caCert.pem -keyfile private/caKey.pem -outdir newcerts/
```

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

5. Enregistrer la clé et le certificat du client du fichier au format PKCS#12

mkdir pkcs12

openssl pkcs12 -export -inkey private/diokhKey.key -in newcerts/diokhCert.crt \
-certfile cacerts/caCert.pem -out pkcs12/diokh.p12

!!! Importer le fichier sur la machine du client

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

6. Apache2 + SSL

sudo a2enmod ssl

sudo systemctl restart apache2

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

6. Apache2 + SSL

Fichier /etc/apache2/sites-available/test-ssl.conf

```
<VirtualHost _default_:443>
ServerName VOTRE_ADRESSE_IP
DocumentRoot /var/www/html
SSLEngine on
SSLCertificateFile    /home/sysadmin/SSL/newcerts/serverCert.crt
SSLCertificateKeyFile /home/sysadmin/SSL/private/serverKey.key
<VirtualHost>
```

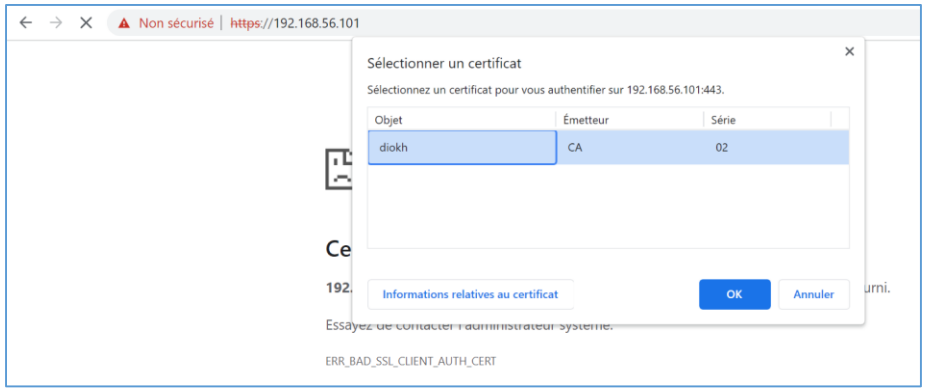
!!! Activer le site avec la commande a2ensite

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

6. Apache2 + SSL + Vérification certificat client



<VirtualHost _default_:443>

....

SSLVerifyClient require

SSLVerifyDepth 10

SSLCACertificateFile /home/sysadmin/SSL/cacerts/caCert.pem

</VirtualHost>

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

7. Création d'un CRL

```
mkdir crl
echo 01 > demoCA/crlnumber
openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -gencrl -crldays 15 -out crl/ca.crl

openssl crl -in crl/ca.crl -text -noout
```

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

8. Révocation du certificat client:

openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -revoke newcerts/diokhCert.crt

mise à jour de la liste des certificats révoqués:

openssl ca -cert cacerts/caCert.pem -keyfile private/caKey.pem -gencrl -crldays 15 -out crl/ca.crl

openssl crl -in crl/ca.crl -text -noout

La signature numérique, les certificats X-509, la notion de PKI

La notion de PKI (Public Key Insfrastructure)

TP: PKI + Apache2: Imposer une authentification basée sur les certificats et gestion de la révocation

9. Apache2 + SSL + Vérification certificat client + gestion de la révocation

<VirtualHost _default_:443>

…

SSLCARevocationCheck chain

SSLCARevocationFile /home/sysadmin/SSL/crl/ca.crl

</VirtualHost>