Master ISIM SIC 1 SID&RS
2013–2014
Chiffrement et authentification
T.T. Dang Ngoc
dntt@u-cergy.fr

TD- Certificats et architecture PKI

1 Définition des AC dans le navigateur

Exercices à faire sur les postes reliés à l'Internet (dans les salles de TP, par Wifi...)

Sur les postes, ouvrez un navigateur (ex : firefox) et :
- affichez la liste des Autorités de Certification par défaut
- Regarder le certificat de l'AC "Comodo Certifica Authority". Qui l'a certifié ?

Affichez le certificat de google.com
- qui l'a certifié ? Construire l'arbre des AC.
- quelle est sa date de validité ?
- quels algorithmes symétrique, asymétrique utilise-t-il ?
- quelle est la classe de l'AE ayant enregistré ce site ? Déduisez en la manière dont a été fait l'enregistrement de ce certificat auprès de l'AE.

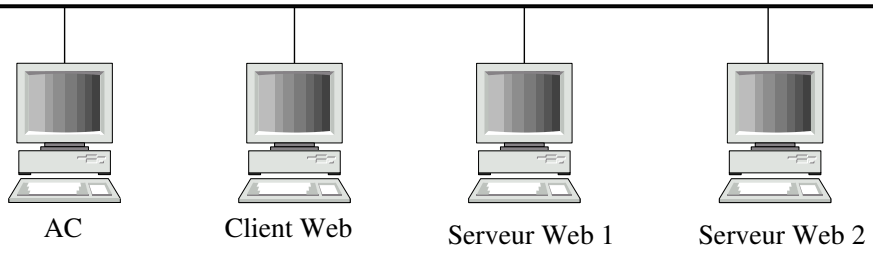
2 Mise en place d'une architecture PKI

Exercices à faire en salle réseaux

Préambule :

Vous configurerez votre installation de la manière suivante :
- Adresse IP : `195.168.236.`*`numéro_de_PC`*
- Adresse de routeur : `195.168.236.254`
- Nom : `pc`*`numéro_de_PC`*`.fournisseur.fr`
- Pas de proxy
- Adresse du serveur DNS : `193.54.113.3`

Vous travaillerez par groupe de deux machines.
- Un PC fera autorité de certification pour un deuxième PC qui sera serveur web
- Vous utiliserez également un client web (un PC d'un autre groupe par exemple) pour les tests.



2.1 Sur l'autorité de certification

Création du certificat de l'autorité de certification

À l'aide de la commande `openssl`, créez une paire de clef privée/publique pour votre machine qui sera autorité de certification.

Entre parenthèses seront indiqués le paramètre correspondant dans le fichier de configuration */etc/ssl/openssl.cnf* à modifier pour s'adapter à vos noms de fichier.

Créez un répertoire `/var/CA` (dir) où vous créerez également les répertoires suivants :
- *certs :* (certs) qui contient les certificats valides
- *crl :* (crl_dir) qui contient la liste des révocations
- *csr :* qui contient les requêtes de certification
- *newcerts :* qui contient les certificats
- *private :* qui contient les clefs privées

Créez également les fichiers suivants :
- *index.txt :* (database) qui contient la liste de tous les certificats de l'AC. (à l'initialisation, créez simplement un fichier `index.txt` vide).
- *serial :* (serial) qui tient à jour le numéro d'index des certificats de l'AC (à l'initialisation, créez simplement un fichier `serial` contenant la ligne 00).
- *crlnumber :* (crlnumber) qui tient à jour le numéro d'index des certificats révoqués de l'AC (à l'initialisation, créez simplement un fichier `crlnumber` contenant la ligne 00).

Modifiez le fichier `/etc/ssl/openssl.cnf` pour positionner la localisation de ces fichiers et répertoires que vous venez de créer.

Création du certificat du site web

À l'aide de la commande `openssl`, générez une clef privée et un certificat pour deux autres machines (deux de vos camarades : `pc`*i*`.fournisseur.fr`) et communiquez les leur.

2.2 Sur le serveur Web

Installez la clef privée et le certificat donnés par votre autorité de certification sur le serveur web.

Emplacement par défaut de la clef privée :
- `/etc/httpd/conf/ssl/server.key` (sous Linux)
- `/usr/local/etc/apache22/server.key` (sous FreeBSD)

Emplacement par défaut du certificat
- `/etc/httpd/conf/ssl/server.crt` (sous Linux)

– `/usr/local/etc/apache22/server.crt` (sous FreeBSD)

2.3 Sur le client Web

Testez sur un client web (`firefox` sur une autre machine) l'accès à la machine :
`https://pc`*num_pc*`.fournisseur.fr`

1. Quelles sont les autorités de certification actuellement supportées par votre navigateur ?
2. Récupérez le certificat de l'autorité de certification ayant validé le certificat des serveurs web. Autorisez l'AC à valider les certificats pour HTTPS.
3. Vérifiez que vous pouvez à présent accéder de manière sécurisée aux serveurs web précédents.

2.4 Révocation

Révoquez un des serveurs web sur l'AC. Publiez la liste de révocation. Chargez la liste de révocation sur le navigateur web. Essayez d'accéder à nouveau aux serveurs web. Vérifiez que le certificat révoqué a effectivement été pris en compte.

2.5 Création du certificat de l'OCSP

À l'aide de la commande `openssl`, créez une paire de clef privée/publique pour la machine qui sera serveur de révocation.

3 Annexe : Configuration réseaux (fichier `openssl.cnf`)

1. *Configurer son interface réseau :* en lui associant l'adresse IP qui vous a été désignée
   ```
   ifconfig <nom_interface> inet <adresse IP> netmask <masque de reseau>
   ```
2. *Configurer sa table de routage :*
   ```
   route add -net <adresse réseau à atteindre> -netmask <masque> <adresse routeur>
   ```
   ou :
   ```
   route add -net <adresse réseau à atteindre>/<CIDR> <adresse routeur>
   ```
   par défaut :
   ```
   route add default <adresse routeur>
   ```
3. *Positionner son nom d'hôte (hostname) :*
   ```
   hostname <nom>
   ```
4. *Déclarer les serveurs de noms :* Pour déclarer les serveurs de noms à utiliser dans la résolution DNS, éditer le fichier `/etc/resolv.conf` (avec la commande `nedit /etc/resolv.conf &` par exemple) et y écrire :
   ```
   nameserver  serveur_de_nom_1
   nameserver  serveur_de_nom_2
   ...
   ```

4 Annexe : Configuration OpenSSL

Génération d'une clef privée

```
openssl genrsa -out clefprivemachine.key 1024
```

Remarque *clefprivemachine.key* de l'AC est spécifié par la variable private_key dans le fichier de configuration sous le nom cakey.pem.

- Si c'est la clef privée de l'AC, elle devra être conservée très très précieusement (bunker informatique) sur l'AC, puisque c'est elle qui garantie tous les certificats émis par cet AC.

- Si c'est la clef privée générée pour une machine dont on éditera le certificat dans les commandes après, elle devra être transmise à la machine en question (par ssh par exemple), et normalement détruite de l'AC.
  Cette clef privée devra être conservée précieusement par son titulaire. Si elle est compromise, le certificat devra être révoqué.

Création du certificat de l'AC

```
openssl req -new -x509 -days nb_jours -key clef_privé_machine.key -out nom_certificat.pem
```

- *nom_certificat.pem est spécifié par la variable certificate dans le fichier de configuration (cacert.pem).*
- Ce certificat sera diffusé publiquement (par exemple en http sur le site web de l'AC, et pourra être chargé par les navigateurs qui souhaitent utiliser cet AC)
- vous n'avez évidemment pas besoin de signer le certificat de l'AC (auto-signé).

Création d'une requête de certification pour une machine

```
openssl req -new -key clef_machine.key -out certificat_machine.csr
```

Attention par défaut, l'AC est configuré pour ne certifier que les machines se déclarant dans la même organisation, région et pays. Afin de passer outre cette limite, vous modifierez match par optional pour les champs countryName, stateOrProvinceName et organizationName dans la rubrique policy_match.

Signature du certificat (sans alias)

```
openssl ca -days nb_jours -in certificat_machine.csr -out certificat_machine.crt
```

Révocation de certificat

```
openssl ca -revoke certificat_machine.crt
```

Génération de la liste de révocation au format PEM puis au format DER

```
openssl ca -gencrl -out crl/liste_pem.crl
openssl crl -in crl/liste_pem.crl -out crl/liste_der.crl -outform DER
```

Cette liste de révocation sera sera diffusé publiquement (par exemple en http sur le site web de l'AC et pourra être chargé par les navigateur qui souhaitent utiliser cette liste de révocation.