POLYTECHNIQUE MONTRÉAL

UNIVERSITÉ D'INGÉNIERIE

INF4420: Éléments de Sécurité Informatique

Exercices Sécurité Web + Corrigé

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité Web

- Exercice 1 : Comprendre l'authentification dans les serveurs Web

- Objectif :
  - Connaître la structure des certificats
  - Comprendre à quoi servent les certificats
  - Comprendre à quoi servent les infrastructures à clé publique (PKI – Public Key Infrastructure)

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Exercices de sécurité Web

- Exercice 1 : Comprendre l'authentification dans les serveurs Web

- Vous souhaitez accéder au site web de votre banque
- Vous saisissez l'URL de votre banque dans votre navigateur
- Votre navigateur fait la demande de connexion avec le serveur de la banque via le protocole HTTPS

Exercices de sécurité Web

- Question 1 : Que se passe-t-il toujours immédiatement après la demande de connexion du client ?

1. Le serveur envoie sa clé de chiffrement symétrique au client
2. Le serveur envoie son certificat au client
3. Le serveur demande au client de s'authentifier
4. Le serveur demande au client de lui envoyer son certificat

Exercices de sécurité Web

- Réponse question 1 : Le serveur envoie son certificat X.509 au client

- Le serveur peut demander son certificat au client
  - C'est optionnel

quand le serveur renvoie son certificat, il contient sa clé publique

ce type de certificat ne fonctionne que si la cryptographie est asymétrique
si on utilise de la cryptographie post quantique il faut trouver un nouveau moyen pour la vérification des certificats

Exercices de sécurité Web

- Question 2 : Qu'est-ce qu'un certificat X.509 ne contient jamais ?
  - La clé publique du serveur
  - La date de validité du certificat
  - La clé symétrique qui va permettre d'établir une connexion sécurisée entre le client et le serveur
  - La signature électronique des informations contenues dans le certificat

client va forger une clé sysmétrique et chiffrer cette clé avec la clé public du serveur et l'envoyer au serveur par la suite le serveur va déchiffrer la clé sysmétrique avec sa clé privée la communication va être chiffré avec la clé symétrique.

chiffrement symmétrique pour communication car meilleur en performance

Exercices de sécurité Web

- Réponse question 2 : Un certificat ne contient jamais la clé symétrique de session

- La clé symétrique pour établir la session sécurisée entre le client et le serveur sera générée ensuite par le client
- Le client utilisera la clé publique transmise par le serveur dans son certificat pour transmettre la clé de session au serveur
- Voir plus tard la présentation du protocole SSL-TSL dans le cours de sécurité réseau 2

Exercices de sécurité Web

- Question 3 : Que fait le client lorsqu'il reçoit le certificat du serveur ?

1. Le navigateur du client consulte sa base de certificats pour vérifier s'il en possède un qui est le même que celui envoyé par le serveur
2. Le navigateur du client consulte sa base de certificats pour vérifier s'il existe une autorité de certification qui confirme la signature du client
3. Le navigateur n'a pas de base de certificats. Il doit envoyer le certificat à une autorité de certification pour vérification

navigateur a une liste de CA root qui émet les certificats
il vérifie si dans le certificat du serveur son root CA est dans sa liste pour confirmer

Exercices de sécurité Web

- Réponse question 3 : Réponse 2
  - Le navigateur du client consulte sa base de certificats (la plupart est intégrée par défaut à l'installation du navigateur)
  - Le certificat envoyé par le serveur annonce une autorité de certification
  - Si le navigateur a le certificat de cette autorité dans sa base, il utilise la clé publique de cette autorité pour vérifier la signature du certificat envoyée par le serveur

- Comment consulter cette base de certificats ?
  - Sous Firefox : Menu → Options
  - Vie privée et sécurité → Certificats → Afficher les certificats

Exercices de sécurité Web

- Structure d'un certificat X.509
  - DN (*Distinguished Name*) de l'entité détentrice du certificat (le serveur)
  - DN du délivreur (autorité de certification)
  - Validité (dates limites)
    - Pas avant
    - Pas après
  - Informations sur la clé publique
    - Algorithme de la clé publique
    - Clé publique proprement dite
  - Divers
    - Numéro de série
    - Algorithme de signature du certificat
    - Version
  - Extensions (optionnel, à partir de X.509v3)
    - Liste des extensions
  - Identifiant unique du signataire (optionnel, X.509v2)
  - Identifiant unique du détenteur du certificat (optionnel, X.509v2)
  - Signature des informations ci-dessus par l'autorité de certification

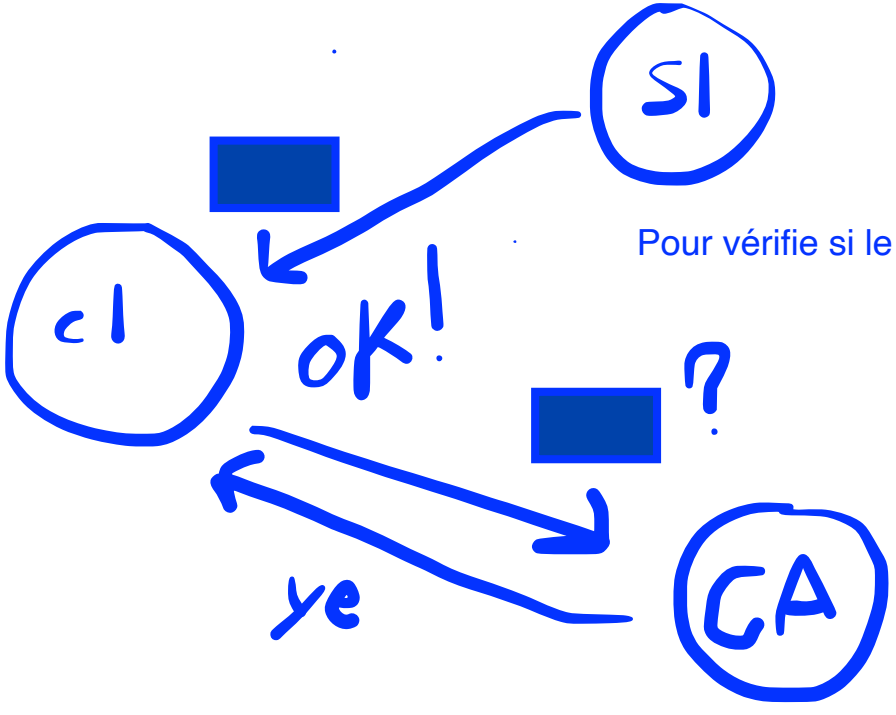
le propriétaire du site génère une paire de clé public et privée et l'envoie a un CA qui va vérifier l'identité du propriétaire. CA va générer un certificat avec la clé publique et d'autres info

client utilise le certificat du server pour générer un hash avec algo SHA-256 et chiffre le hash avec la clé public du CA trouvé avec un algo comme RSA et compare le resultat avec la signature du certificat

Exercices de sécurité Web

- Question 4 : Une fois que le navigateur du client a vérifié que le certificat du serveur est signé par une autorité valide, le client va consulter cette autorité de certification ?

1. Vrai
2. Faux



Pour vérifie si le certificat n'est pas révoqué

CA garde une liste de certificats révoqués

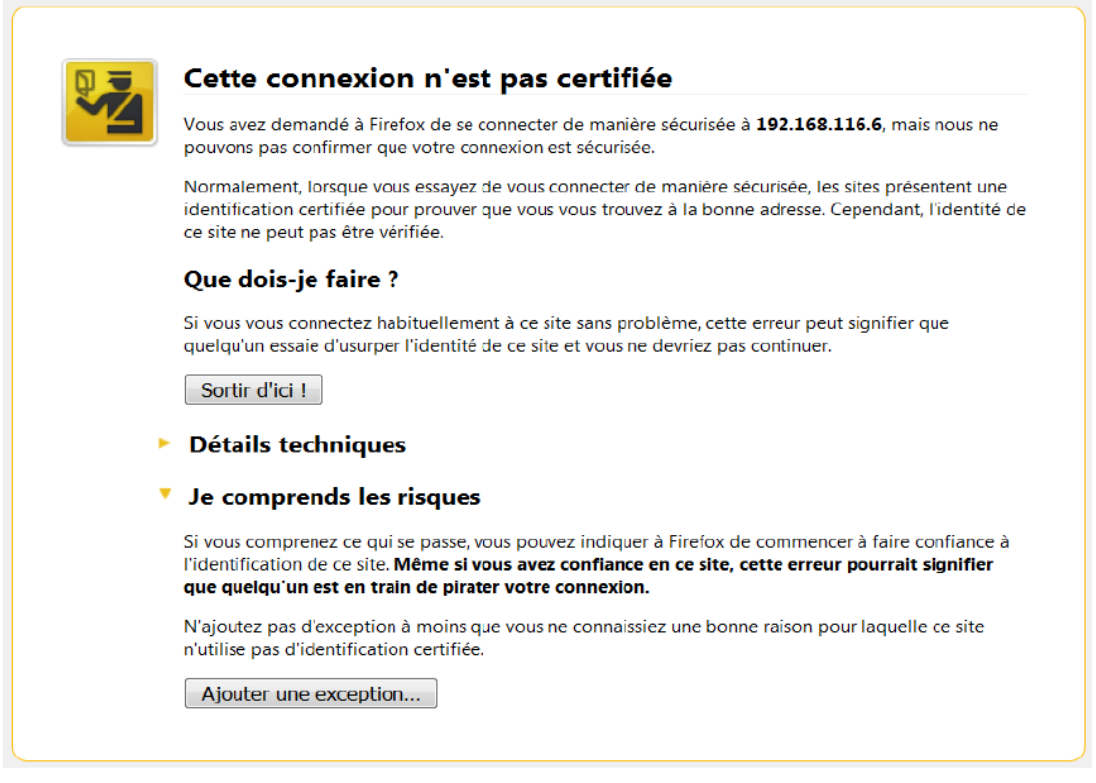
Exercices de sécurité Web

- Réponse question 4 : C'est vrai

- Le client demande à l'autorité de certification de confirmer que le certificat n'a pas été révoqué par l'autorité

Exercices de sécurité Web

- Remarque : il peut arriver que certains sites utilisent leur clé privée pour signer leur certificat
  - On parle alors de certificat auto-signé
  - En général, c'est une anomalie que votre navigateur va vous signaler
  - A vous de décider ! (soyez prudent)



Exercices de sécurité Web

- Hiérarchie d'autorités de certification et autorités racines
  - Certaines autorités de certification jouent le rôle d'autorités racines
  - Ce sont les seuls certificats qui devraient pouvoir être auto-signés
- Exemple de certificats racines installés par défaut :
  - VeriSign
  - Entrust.net
  - Equifax Secure
  - GlobalSign
  - GTE CyberTrust Root et Global Root
  - Secure Server (RSA)
  - Thawte Premium Server

certificat chainé si entreprises avec ses filiales ou objets connectés

CA émet un certificat pour un CA intermédiaire qui à son tour va signer un certificat à un site

Client vérifie le CA root et descend jusqu'à la fin
si un dans chaîne foire tout foire

Exercices de sécurité Web

- Conséquence 1
  - Le serveur n'a peut-être pas un certificat signé par une autorité racine
  - Dans ce cas, c'est une chaine de certificats remontant jusqu'à une autorité racine que le serveur doit envoyer au client
  - Le client doit vérifier tout la chaine pour valider le certificat du serveur
  - On parle alors de certificats chainés

Exercices de sécurité Web

- Conséquence 2 et question 5 : Que se passe-t-il si une autorité de certification se fait voler sa clé privée ?
  1. Game over !
  2. Il faut réinstaller le navigateur
  3. L'autorité doit immédiatement révoquer tous ses certificats
  4. L'autorité et toutes les autorités ayant des certificats chainés avec cette autorité doivent révoquer leurs certificats

relation hierarchique CA peut prévenir
Bob (serveur)

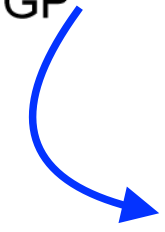
Exercices de sécurité Web

- Réponse question 5 : Réponse 4
  - Si une autorité se fait voler son certificat, c'est toute la chaine de certificats issues de cette autorité qui est potentiellement corrompue !
  - C'est pourquoi il est très important que le client vérifie auprès de l'autorité de certification que le certificat n'a pas été révoqué

Exercices de sécurité Web

- Infrastructures de Gestion de Clés (IGC)
  - En Anglais : Public Key Infrastructure (PKI)

- Une autorité de certification est un cas particulier d'IGC
  - Modèle de PKI reposant sur les certificats X.509
  - Il existe d'autres modèles de PKI notamment PKI distribuée
    - Toile de confiance avec OpenPGP
    - Blockchain-based PKI



plusieurs noeuds chaque recommende la confiance pour un autre