Comodo, les géants face aux intrusions

D'après un article de la revue ActuSécu. No 28. XMCO.

Introduction

Comodo est un pilier de la sécurité sur Internet. L'entreprise propose une large gamme de produits et de services destinés à protéger les données des internautes. Comodo est également une entreprise proposant de nombreux produits de sécurité : firewall, certificats SSL, e-mail signé, outils de sécurisation de sites Web, authentification, chiffrement, etc. Plus de 2 millions de certificats numériques signés par Comodo ont été installés. Enfin Comodo joue un rôle d'autorité de certification (CA) qui s'appuie sur un réseau d'autorités d'enregistrements (RA) indépendantes réparties à travers le monde. Ce sont ces dernières qui effectuent les vérifications d'identités nécessaires à l'émission d'un certificat.

http://www.comodo.com/

Le 31 mars 2011, l'autorité de certification Comodo a officiellement déclaré avoir été compromise 15 jours auparavant...

Exercice 1 : certificat, Autorité de certification, https

... L'attaque visait plus précisément l'autorité d'enregistrement (RA) InstantSSL.it située en Italie et affiliée à Comodo. Le pirate aurait compromis un compte utilisateur de cette RA et aurait ainsi généré frauduleusement neuf certificats de sécurité valides pour des noms de domaines majeurs tels que Gmail, Mozilla, Skype, ou encore Yahoo.

Avant d'aller plus loin, quelques questions de rappel.

Un administrateur souhaite obtenir un certificat signé par une autorité de certification (CA) pour un serveur web. Il va donc générer une requête de signature RCS, adressée à une autorité d'enregistrement, et comprenant plusieurs champs.

- 1.1. Quelles sont les informations composant cette requête ?
- 1.2. Commentez les lignes suivantes :
    - *openssl genrsa -out server.key 2048*
    - *openssl req -new -in server.key - out certificat.req*
- 1.3. Que fait le CA une fois que cette demande de certificat lui est parvenue ?
- 1.4. Quelles sont les informations transmises à l'administrateur par le CA ?

- 1.5. Quelles sont ensuite les étapes réalisées par le navigateur du client se connectant sur ce serveur en https ? *Remarque : soyez précis dans les étapes réalisées.*
- 1.6. Donnez une explication au message d'erreurs affiché par le navigateur (voir ci-dessous). *Remarque : il s'agit ici d'un contexte différent des cinq premières questions.*

➔ *Connexion au site web*

> *Message d'erreur affiché: Impossible de vérifier l'identité du site web comme site fiable. Signalez ce problème à l'administrateur du site. Avant d'accepter le certificat de ce site, étudiez-le attentivement. Voulez-vous acceptez ce certificat comme identification du site Web?*

- 1.7. Commentez le schéma de la figure 1 permettant l'établissement d'une connexion sécurisée avec le site web.

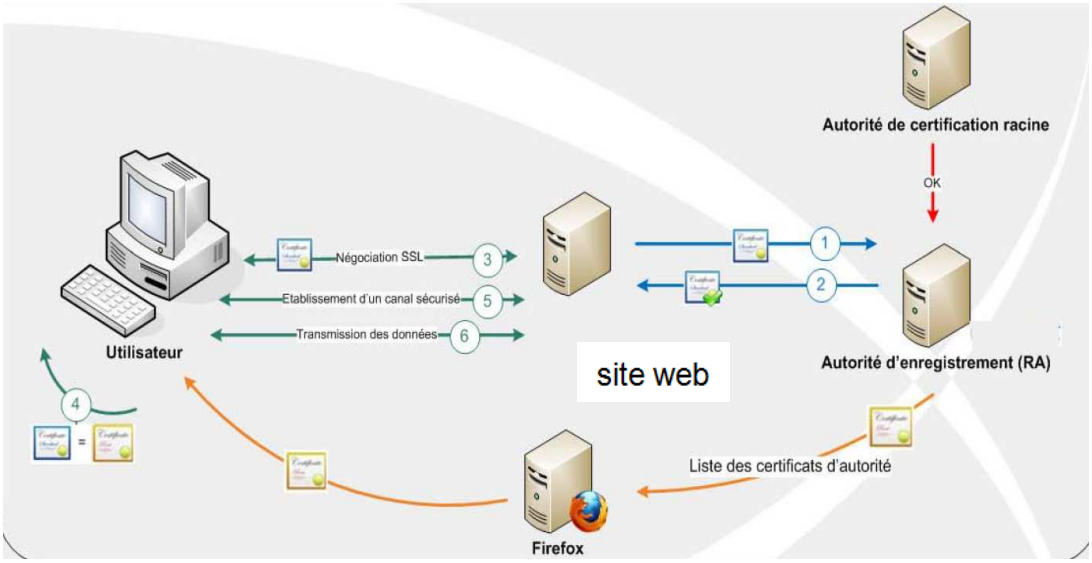


Figure 1. Principe de l'établissement d'une connexion sécurisée

Exercice 2 : attaques sur une autorité de certification

Pour prouver qu'il était bien l'auteur de cette attaque, le pirate n'a pas hésité à publier la clé privée et le certificat frauduleux, relatif à la plateforme de téléchargement d'extensions de Mozilla : addons.mozilla.org (cf. fig.2).

Figure 2. Certificat et clé privée associée

Nous souhaitons vérifier les dires du hacker. Pour ce faire nous utilisons l'utilitaire en ligne de commande Openssl qui possède les différentes fonctions cryptographiques dont nous avons besoin. Remarque : texte_test est un fichier contenant un texte en clair.

- 2.1. Expliquez les lignes de commande suivante et leur objectif :
openssl x509 -noout -inform DER -in addons.mozilla.org.cer -pubkey > public .pem
openssl rsautl -encrypt -inkey public.pem -pubin -in texte_test -out encrypted
openssl rsautl -decrypt -inkey private.pem -in encrypted -out texte_test1
cat texte_test1

x509 :	Utilitaire pour gérer un certificat. X.509 est un format standard de certificat électronique.
rsautl :	Utilitaire RSA utiliser pour signer, vérifier, chiffrer et déchiffrer.
noout :	Supprime la sortie standard normalement produite.
inform DER :	Format particulier correspondant à une structure PKCS#7 v1.5, c'est-à-dire ne prenant pas en compte les commentaires en en-tête et pied de page.
encrypt/decrypt :	Pour spécifier le mode utilisé.
inkey :	Pour indiquer l'endroit où se situe la clé.
pubin :	Pour spécifier que le fichier ne contient que la clé publique.
in :	Fichier d'entrée.
out :	Fichier de sortie.

La deuxième vérification est effectuée par la ligne suivante (l'AC de Comodo est UTN-UserFirst):
openssl verify -CAfile UTN-USERFirst-Hardware addons.mozilla.org.pem
- 2.2. Expliquez l'objectif de cette vérification.

Scénarios d'attaque

A. Nous considérons le scénario d'attaque numéro 1 décrit par la figure 3.

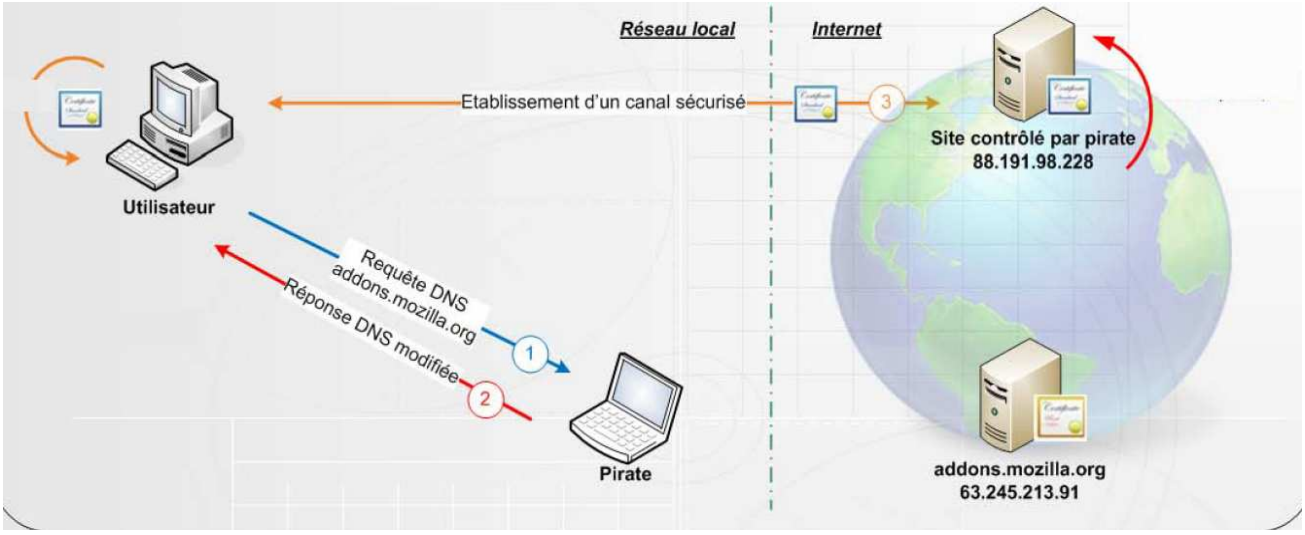


Figure 3. Scénario 1
Remarque : on considère que le serveur DNS se trouve sur le même sous-réseau que la victime.

- 2.3. Décrivez avec précision l'ensemble des actions que doit entreprendre le pirate pour mettre en œuvre cette attaque. Que peut faire le pirate pour inciter l'utilisateur à se connecter sur le site d'addons ? Sur quel protocole repose cette attaque?
- 2.4. Décrivez également l'ensemble des actions qu'entreprend le système/le navigateur de l'utilisateur. Pour quelle raison cette attaque a toutes les chances de fonctionner dans le cadre d'un réseau privé ?

B. Nous considérons maintenant le scénario d'attaque numéro 2 décrit par la figure 4, Quelle différence y a t-il avec le premier scénario ? Comment s'appelle cette attaque ?

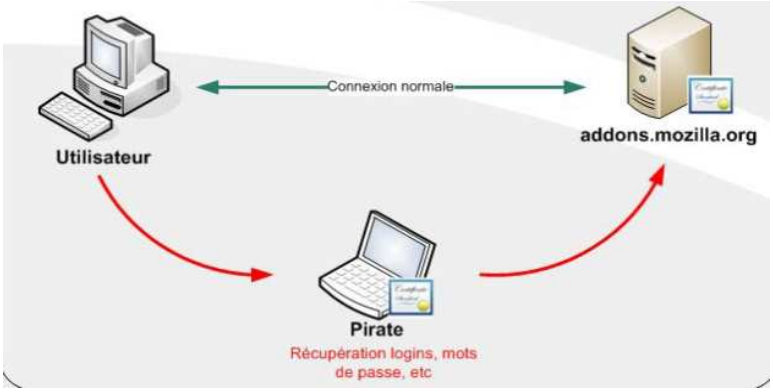


Figure 4. Scénario 2

- 2.5. Comment se protéger ?

Sécurité de la dématérialisation

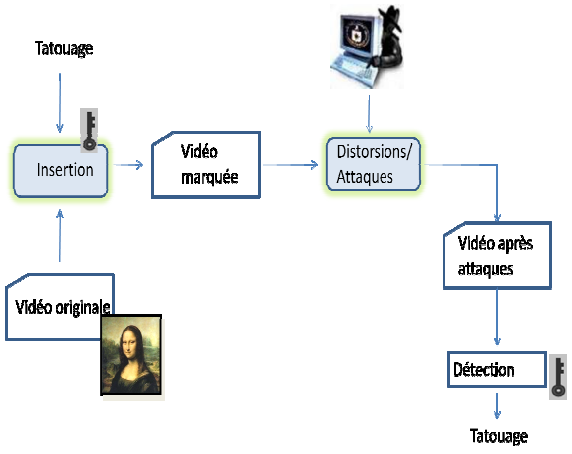
Exercice 3 : Protocoles de sécurité

Précisez sous la forme d'un schéma commenté un protocole permettant de préserver :

- la confidentialité des données
- l'intégrité des données
- l'authentification de l'émetteur et de l'expéditeur
- la non-répudiation

Précisez le rôle d'une autorité de certification dans ce protocole de sécurité

Exercice 4 : Protection des droits d'auteur. Watermarking



Décrivez sous la forme d'un schéma commenté précisément un algorithme de tatouage d'images permettant :

- de vérifier l'intégrité forte de celle-ci (Hash),

- et d'insérer un logo,

Autrement dit, le schéma de tatouage doit dire si l'image a été modifiée. Le Logo et une clé seront utilisés et permettront de vérifier l'intégrité.

Exercice 5 : RSA

Soit p et q deux nombres premiers. Nous définissons de plus n=pq, et la fonction indicatrice d'Euler $\phi(n) = (p-1)(q-1)$.

Soit e entier choisi premier avec $\phi(n)$, et soit d l'inverse de e modulo $\phi(n)$

1. Pour p=3 , q=11, calculez n et $\phi(n)$.
2. Soit e=7. Calculez d à partir de l'équation $e.d=1 \mod \phi(n)$ (utilisez l'algorithme d'Euclide étendu).
3. Donnez l'équation de chiffrement d'un message M.
4. Donnez l'équation de déchiffrement.
5. Quel est la clé publique, quel est la clé privée ?
6. Sur quel principe reposent les attaques par force brute ?