Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

*Master 1ère année*

*UE Sécurité des Usages TIC*

**Examen — mai 2012**

*Durée : 2h — Tous documents autorisés*

**1 – 15 pts** Article paru dans SecurityVibes :
`http://www.securityvibes.fr/menaces-alertes/diginotar-attaque-certificats/`

**DigiNotar : une affaire plus complexe qu'il n'y parait**

*Auteur de l'article : Jérôme Saiz le 5 septembre 2011 - 15:42, dans la rubrique Alertes & Menaces*

Vous pensiez que l'affaire du piratage de DigiNotar s'arrêtait à un vrai-faux certificat émis au nom de Google ? La vérité va bien au delà et implique désormais même une PKI gouvernementale.

Ce sont en réalité 247 certificats qui semblent avoir été générés par les pirates, pour 23 noms de domaine différents. Ceux-là avaient cependant une durée de vie très courte et expiraient le 19 août 2011. Ils ne sont donc plus utilisables désormais même s'ils n'ont pas étés officiellement révoqués. On trouve parmi eux les noms de domaines d'agences de renseignement occidentales (CIA, MI6 et Mossad). Un acte inutile qui peut être interprété comme un pied-de-nez ou la marque d'une grande naïveté : les informations confidentielles manipulées par ces agences empruntent très certainement un réseau distinct de l'internet public, où ces certificats sont totalement inutiles.

Mais un autre certificat, intermédiaire, a été émis une semaine avant ceux-ci. Un certificat intermédiaire est utilisé pour signer d'autres certificats en leur conférant la confiance envers son organisme émetteur. Celui-ci est encore valable, et c'est notamment lui qui a servi à générer le fameux vrai-faux certificat pour *.google.com.

Mais ce sésame intermédiaire pouvait être utilisé pour générer bien d'autres certificats que celui de Google. Ne disposant d'aucune archive le concernant, DigiNotar ne peut dire combien d'autres vrais-faux certificats similaires à celui de Google circulent actuellement, et il lui est donc bien entendu impossible de les révoquer.

D'après un ingénieur de la Fondation Mozilla, il y en aurait au moins quatre, mais probablement beaucoup plus. La méthode utilisée pour tenter de les détecter est en effet loin d'être idéale : elle consiste à rechercher des numéros de série inconnus dans les requêtes de révocation émises par certains navigateurs lorsqu'ils rencontrent un certificat. Autant dire qu'il s'agit au mieux d'une pêche à grandes mailles. . .

(*Suite et fin de l'article au verso.*)

Dans le doute, la majorité des navigateurs ont désormais pris des mesures pour désactiver tous les certificats de DigiNotar, sans distinction : nouvelles versions pour Chrome et Firefox notamment et une mise à jour Windows pour Internet Explorer (uniquement pour les utilisateurs de Vista et Seven pour l'instant). Une telle mesure est exceptionnelle et radicale, à la hauteur de cette affaire. Chez Mozilla, par exemple, les développeurs ont ajouté du code chargé de détecter le nom de DigiNotar et d'interdire purement et simplement la visite de sites qui en ferait usage, sans offrir à l'utilisateur la possibilité de contourner le blocage (uniquement pour les certificats émis après le 1er juillet 2011).

L'analyse de cette attaque est compliquée par de très nombreuses bourdes de la part de DigiNotar : les journaux d'activité sont parcellaires, les certificats vendus par la société ne contenaient souvent pas d'informations de révocation, ses ingénieurs n'ont pas découvert la fuite du certificat intermédiaire malgré six semaines d'enquête et son site web aurait été piraté en 2009 sans qu'elle ne s'en rende compte… Pire : d'après le document publié par un ingénieur en charge de la coordination entre DigiNotar et la Fondation Mozilla, des certificats frauduleux continuaient à être émis un jour après la découverte du piratage par les équipes de DigiNotar. Autant de bourdes ont d'ailleurs valu à Vasco, la maison-mère de DigiNotar, d'être récemment malmenée en bourse.

Mais là où l'affaire prend un tour plus institutionnel, c'est lorsque l'on apprend que des certificats racines émis par DigiNotar chapeautent la PKI opérée par le gouvernement hollandais, utilisée aussi bien en interne qu'en externe et notamment pour authentifier les citoyens en ligne (projet DigiID, basé sur le numéro de sécurité sociale).

Le blocage des certificats de DigiNotar menaçait donc d'interdire l'accès à la PKI du gouvernement Hollandais. Ce dernier avait pourtant initialement indiqué, via son propre CERT, que les deux certificats racines de sa PKI étaient distincts de l'infrastructure mise en cause chez DigiNotar, et avait alors demandé à bénéficier d'une exception… qui lui a tout d'abord été accordée. Mais il semble qu'un audit mené par une entreprise tierce ait déterminé que le risque de fraude existait malgré tout : la PKI du gouvernement a donc du se trouver un autre fournisseur dans l'urgence. Il semblerait qu'il s'agisse maintenant de QuoVadis.

Les auteurs de cette opération ne sont pas connus. Tout porte à croire qu'il s'agit de pirates iraniens. Ont-ils oeuvré pour le compte du gouvernement ou par patriotisme ? Impossible de le déterminer. Il est même possible qu'il y ait eu plusieurs groupes de pirates, indépendants les uns des autres, tant l'attaque qui a permis la création du certificat intermédiaire – et son exploitation hors du contrôle de DigiNotar – est plus subtile que la génération massive de 247 certificats directement sur la plate-forme de l'opérateur.

a. Dans le paragraphe 2 de l'article, de « *Ce sont en réalité 247 certificats. . .* » à « *. . . où ces certificats sont totalement inutiles* », l'auteur parle de « *nom de domaines* », de « *durée de vie* » *etc.* :
   - ◇ précisez à quels champs du certificat cela correspond ;
   - ◇ est-ce normalisé ?

   ***1 pt***

b. L'article parle de « *PKI gouvernementale* » :
   - ◇ expliquez le terme de « *PKI* » ;
   - ◇ à quoi correspond le type « *gouvernementale* » ?
   - ◇ connaissez vous d'autres exemples de ce type et leur utilisation ?

   ***1 pt***

c. Comme indiqué dans l'article, une réponse à des attaques est fournie par le CERT :

> **CERT**
>
> *En sécurité informatique, il existe des organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT (Computer Emergency Response Team) sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous (souvent au travers d'un site Web).*

   - ◇ quelles sont les autres réponses fournies automatiquement par votre système d'exploitation ?
   - ◇ quelle est, à votre avis, la stratégie la plus efficace ?

   ***1 pt***

d. Dans le paragraphe « *Dans le doute, la majorité des navigateurs ont. . .* » à « *. . . uniquement pour les certificats émis après le 1$^{er}$ juillet 2011)* »
   - ◇ en tenant compte du fait que la PKI est décomposée en différentes entités, et par rapport à la solution apportée par Mozilla, quelle a été la cible et la portée de l'attaque permettant de générer un certificat ?

   ***1 pt***

e. Le titre de l'article parle de « *vrais-faux certificats* », expliquez de quoi il s'agit.
   ***1 pt***

f. Expliquez la hiérarchie des certificats dont l'article parle et pourquoi l'attaque sur le **seul certificat** « google » est plus dangereuse que sur les **247 autres certificats** ?
   ***2 pts***

g. Le caractère « ∗ », appelé *wildcard*, peut se substituer à toute chaîne de caractères :
   - ◇ son utilisation dans un certificat est-elle dangereuse ?
   - ◇ expliquez les risques et, en particulier, pour un logiciel client.

   ***1 pt***

h. Qu'est-ce qu'un « certificat racine » et pourquoi la réponse du « *gouvernement Hollandais* » n'était pas suffisante ?
   ***2 pts***

i. Donnez 3 méthodes de blocage de certificat.
   *Toutes ces méthodes sont évoquées dans l'article*
   ***1 pt***

j. Dans le paragraphe « *D'après un ingénieur de la Fondation Mozilla. . .* » à « *. . . au mieux d'une pêche à grandes mailles. . .* », l'article parle de « *requête de révocation* » :
   - ◇ à quelle technologie fait-il référence ?
   - ◇ en quoi cette méthode est-elle différente du téléchargement de la liste de révocation ?
   - ◇ expliquez comment cette technologie peut permettre d'identifier les « *vrais-faux certificats intermédiaires* » ?

   ***2 pts***

k. Pourquoi l'attaque est considérée comme « *courte* » et semble un « *pied de nez* » ou « *la marque d'une grande naïveté* » ?
***1 pt***

l. Qu'est-ce qui identifie une entité dans un certificat x509 et qu'est-ce que le projet DigiID apporte comme amélioration ?
***1 pt***

## ▬▬▬ Questions indépendantes de l'article

**2 – Certificat** :

**1pt** a. Est-il possible de créer plus d'un certificat pour une même entité ?

b. Si deux certificats existent pour une même entité, quelles sont les différences entre ces deux certificats ?

c. Quelle information est nécessaire pour révoquer un certificat ?

**3 – Connexion SSL** :

**1pt** a. en quoi une connexion SSL peut-elle amener de la sécurité ?

b. est-elle susceptible d'être écoutée par un tiers non autorisé (attaquant) ?

**4 – OCSP** :

**1pts** a. Pourquoi faut-il authentifier la réponse OCSP ?

b. auprès de qui ?

**5 –** Expliquez le concept de « ***passphrase*** » :

**2pts** a. à quoi sert-il ?

b. quelles différences avec une clé de chiffrement ?

c. qu'est-ce qu'apporte le concept de « *salt* » ?