Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

Sécurité des Usages TIC

Examen — mai 2013

Durée : 2h — Tous documents autorisés

1 – 16 pts Article paru dans InterCloud :
`https://www.intercloud.fr/actualites/rsa-2013-pour-les-experts-se-preparer-au-post-crypto/`

Pour les experts, il est temps de se préparer à un monde «post-Crypto »

Auteur de l'article : Denis Fisher, ***Conférence RSA 2013****, 27 février 2013*

Dans un climat actuel où les attaques et les intrusions orchestrées par des groupes soutenus par des gouvernements ou autres organisations s'intensifient, la cryptographie devient de moins en moins importante et les experts en sécurité doivent commencer à réfléchir à de nouvelles façons de protéger les données sur des systèmes qu'ils supposent compromis. Adi Shamir, qui a participé à la conception de l'algorithme original de RSA, a même déclaré que les experts en sécurité devraient se préparer à une ère « post-cryptographie ».

Shamir, qui faisait partie du panel d'experts au RSA 2013 avec Ron Rivest du MIT, Dan Boneh de l'Université de Stanford, Whitfield Diffie de l'ICANN et Ari Juels du centre de recherche de RSA, a déclaré que les agressions, de plus en plus sophistiquées, contre les réseaux d'entreprises et de gouvernements sont devenues l'événement le plus important dans le monde de la sécurité. Le temps est venu pour les chercheurs en sécurité et pour ceux impliqués dans la défense des réseaux de mettre au point de nouvelles méthodes différentes de la cryptographie et qui seront efficaces dans la sécurisation des données sensibles.

« Nous avons besoin d'une Infrastructure à Clé Publique (PKI : Public Key Infrastructure) où nous pourrions choisir les entités à qui nous faisons confiance, mais nous n'avons pas encore cette capacité » a déclaré Rivest, un des co-auteurs de l'algorithme RSA. « Nous avons vraiment besoin d'une Infrastructure à Clé Publique qui ne soit pas seulement flexible dans le sens où les participants puissent choisir en quoi ils ont confiance, mais aussi dans le sens d'être capable de tolérer des problèmes qu'ils soient accidentels ou dus à une intervention d'un gouvernement. Nous avons encore une approche naïve des Infrastructures à Clé Publique, nous devons absolument approfondir ce sujet. »

Shamir a pointé un incident qui est survenu récemment, dans lequel TurkTrust, une autorité de certification turque, a délivré des certificats pour les domaines Google à deux entités, l'une d'elle étant un prestataire du gouvernement Turc. Shamir ne serait pas surpris de voir ce genre d'incident apparaître à nouveau : « Je pense que vous verrez de plus en plus d'événements de ce genre, où une AC, sous la pression d'un gouvernement, se comporte de façon étrange. C'est à se demander si la base de la sécurité, les infrastructures à clés publiques, n'atteindrait pas ses limites. »

La conférence RSA est une série de conférences portant sur la sécurité de l'information. Principalement destiné aux industriels, les conférences sont organisées à la fois aux États-Unis et en Europe, tous les ans depuis 1999.

Un bulletin d'alerte a été publié sur le site Web du CERTA de l'ANSSI accessible à l'adresse suivante : `http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-001/`

> Un nouvel incident remettant en question le modèle actuel de gestion des certificats a récemment été constaté. Google a annoncé avoir découvert un certificat valide ne leur appartenant pas pour le domaine « *.google.com ». Ce certificat frauduleux a été émis par une autorité de certification (AC) intermédiaire, elle-même certifiée par une AC racine turque TURKTRUST.
> Toujours selon Google, TURKTRUST aurait reconnu avoir délivré par erreur, en août 2011, deux certificats d'AC intermédiaires au lieu de certificats finaux à des organisations. Ces organisations, ou tout utilisateur ayant accès aux clés privées associées à ces certificats, ont donc eu la possibilité de créer des certificats valides pour n'importe quel site Web.
> En plus de Google qui a révoqué les certificats concernés, Microsoft a publié une mise à jour pour ses systèmes. Les systèmes utilisant la mise à jour automatique de certificats révoqués, incluant Windows Vista et supérieurs ou Windows Server 2008 et supérieurs, devraient recevoir la mise à jour automatiquement. Par contre, les administrateurs des systèmes plus anciens dont Windows XP et Windows Server 2003, doivent passer par Windows Update ou appliquer la mise à jour manuellement (se référer au bulletin de sécurité Microsoft pour de plus amples détails).
> Mozilla a annoncé une mise à jour pour Firefox qui sera disponible le 8 janvier 2013.
> Le CERTA recommande l'application des mises à jour concernant ces certificats dès que possible.

a. L'article d'InterCloud parle de « *l'algorithme RSA* », à quoi sert-il ?
   1pt

b. Comment s'établit la confiance dans une PKI et quel rôle joue l'« Autorité de Certification » ?
   2pts

c. Pourquoi un système d'exploitation connaît-il le certificat de TurkTrust et le considère-t-il comme une « Autorité de Certification » ?
   Quelles sont les particularités de ce type de certificat (dans les champs qui le composent) ?
   2pts

d. Qu'est-ce qu'une « AC intermédiaire » ?
   Quelles sont ses capacités ?
   En connaissez vous une ?
   2pts

e. Quelles attaques sont rendues possibles par l'utilisation de ce type de « certificat frauduleux » ?
   Est-ce qu'il existe des outils de protection automatique contre ces attaques ?
   1pt

f. Comment amener le navigateur d'une personne à utiliser le « certificat frauduleux » lors de la connexion à un site ?
   1pt

g. Quel protocole de communication utilise un « certificat » et pour quel usage ?
   Quelles sont les étapes que va utiliser le navigateur Web pour accéder un site situé dans le domaine `google.com` et de quelles manières le certificat émis par TurkTrust sera utilisé à la place de celui officiel ?
   1pt

h. À partir de votre expérience acquise lors des séances de TPs, quelle procédure appliqueriez vous pour éviter de tomber dans ce piège ?
   1pt

i. À votre avis, la découverte de l'existence de ce « certificat frauduleux » a-t-elle été facile ?
   1pt

j. Dans les réponses décrites dans le bulletin d'alerte fourni 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).*
> *En France, l'ANSSI, « Agence nationale de la sécurité des systèmes d'information » propose un service identique nommé CERTA, « Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques » accessible sur son site Web.*

   - ◇ Quelles sont les deux types de réponses à cette alerte ?
   - ◇ Quelle est, à votre avis, la stratégie la plus efficace ?
   - ◇ Est-ce qu'OCSP aurait aidé dans ce cas ?

   2pts

k. Dans le paragraphe 3 de l'article, Ron Rivest parle de « *. . . choisir les entités à qui nous faisons confiance. . .* »
   - ◇ Expliquez ce qu'il veut dire ?
   - ◇ Pouvez vous donner des pistes pour corriger le problème ?

   2pts

▬▬▬ Questions indépendantes de l'article – 4 points

2 – 2pts D'après Wikipedia :

> **DNSSEC**
>
> *DNSSEC permet de sécuriser les données envoyées par le DNS. Il sécurise les enregistrements DNS échangés par le serveur DNS même lorsque ces enregistrements sont fournis par un serveur DNS intermédiaire malveillant.*
> *DNSSEC signe cryptographiquement les enregistrements DNS et met cette signature dans le DNS. Ainsi, un client DNS méfiant peut récupérer la signature et, s'il possède la clé du serveur, vérifier que les données sont correctes.*
> *DNSSEC permet de déléguer des signatures : ainsi, le registre d'un domaine de premier niveau, « Top Level Domain », peut annoncer que tel sous-domaine est signé. On peut ainsi bâtir une chaîne de confiance depuis la racine du DNS.*
>
> `http://fr.wikipedia.org/wiki/Domain_Name_System_Security_Extensions`

a. Comment se met en place la confiance avec DNSSEC lorsqu'un utilisateur demande l'adresse IP du serveur « `www.unilim.fr` » par rapport aux DNS gérant le domaine « `unilim` » et « `fr` » ?
b. Est-ce que ce système permet d'éviter les attaques « *Man-In-The-Middle* » ?

3 – 1pt **Certificat** :

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 ?

4 – 1pt Dans l'OTP proposé par les services fournis par Google :

a. Pourquoi le mot de passe que l'on utilise pour se connecter à son compte Google est différent du secret utilisé par l'OTP ?
b. Existe-t-il quand même un lien ?