Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

UE Sécurité des Usages TIC

Examen — mai 2011

Durée : 2h — Tous documents autorisés

1 – 10pts Dans un article du site d'information « ZDNet.fr », publié le 24 mars 2011, le journaliste Christophe Auffray relate l'attaque survenue sur la société Comodo :

Des Certificats SSL Frauduleux De Comodo Autorisent Des Attaques Contre Les Webmails

***Sécurité* - Neuf certificats SSL ont été générés frauduleusement grâce à une intrusion informatique sur le service d'une autorité de certification. Les principales messageries, dont Yahoo Mail, Gmail et Hotmail étaient visées. La motivation serait politique, ces certificats devant permettre de leurrer des internautes et d'accéder à leurs courriels.**

L'autorité de certification Comodo, qui délivre donc des certificats SSL, a déclaré qu'une intrusion informatique réussie avait visé un de ses affilés via la compromission d'un compte utilisateur. Cette attaque a ainsi permis de générer frauduleusement 9 certificats SSL, concernant 7 domaines.

Ces certificats portent sur les principaux services de messagerie électroniques, à savoir Yahoo Mail, Hotmail et Gmail, mais également Skype, la plate-forme de téléchargement d'extensions de Mozilla et Global Trustee.

Un piratage en plein mouvement de contestation au Maghreb et dans le Golfe

La détention de tels certificats permet à des pirates de réaliser différentes attaques, en leurrant le navigateur Web, et notamment de type phishing en usurpant l'identité d'un site légitime comme Gmail ou Live Messenger.

Sur son blog, Comodo indique que les certificats frauduleux ont tous été révoqués. Microsoft a d'ores et déjà publié un bulletin d'alerte et diffuse via Windows Update une mise à jour actualisant la liste des certificats révoqués sur Windows.

Les principaux navigateurs prennent également des mesures afin de prévenir des attaques exploitant ces certificats. C'est notamment le cas pour Chrome et Firefox. Mozilla a confirmé avoir placé les certificats SSL en liste noire :

« Les utilisateurs d'un réseau compromis pouvaient être redirigés vers des sites utilisant des certificats frauduleux se faisant passer pour des sites légitimes. Cela pouvait les tromper et les amener à dévoiler des informations personnelles, comme des identifiants et des mots de passe »

Cette usurpation d'identité pouvait également les trahir et ainsi les conduire à télécharger, en toute confiance, du code malveillant précise encore Mozilla.

Source : `http://www.zdnet.fr/actualites/des-certificats-ssl-frauduleux-de-comodo-autorisent-des-attaques-contre-les-webmails-39759360.htm`

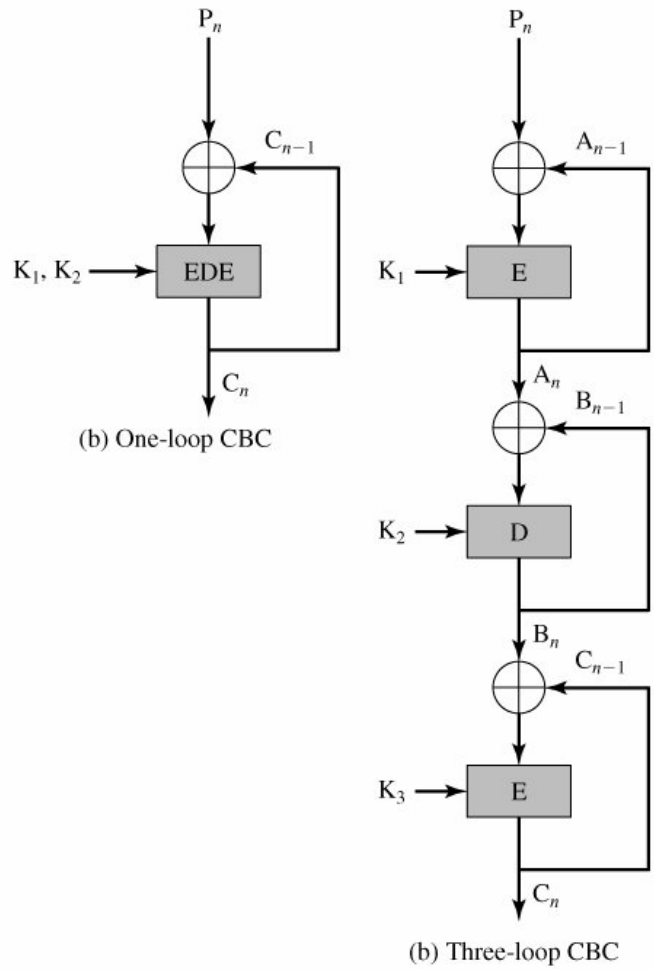
P_n
C_{n-1}
K_1, K_2
EDE
C_n
(b) One-loop CBC
P_n
A_{n-1}
K_1
E
A_n
B_{n-1}
K_2
D
B_n
C_{n-1}
K_3
E
C_n
(b) Three-loop CBC

Figure 1

a. Quelle sorte de service offre Comodo ?

b. Qu'est-ce que le protocole « HTTPS », comment fonctionne-t-il ?
Quelles sont les différences de traitement entre des sites connus comme ceux attaqués (Gmail, Hotmail et Yahoo mail) et un site que vous auriez sécurisé vous-même ?
Pourquoi le système de l'utilisateur n'est pas capable de détecter l'attaque ?

c. Le journaliste parle de « *compromission d'un compte utilisateur* » de « *un des affiliés* » de « *l'autorité de certification* », ce qui est précisé par le journaliste Jérôme Saiz du site « SecurityVibes » :
« *Les certificats sont produits à la demande par l'américain Comodo, qui s'appuie sur un réseau d'autorités d'enregistrement (RA) indépendantes réparties à travers le monde. Ce sont elles qui opèrent sur le terrain les vérifications d'identité nécessaires à l'émission d'un certificat, et c'est l'une de ces dernières, en Europe, qui aurait été compromise. L'attaquant aurait alors demandé à générer neuf certificats pour des domaines majeurs, quasiment tous dans le domaine des communications (email et téléphonie sur internet).* »
Expliquez brièvement comment se déroule la création du certificat avec les différentes autorités : quels sont les éléments cryptographiques qui sont échangés et sous quel format ?

d. Expliquez comment, à votre avis, l'attaquant a pu s'y prendre pour accéder au compte ?
Donnez au moins deux moyens d'y parvenir.

e. Est-ce que cette attaque permet de remplacer des certificats déjà émis ?

f. Est-ce que cette attaque signifie que l'architecture de la PKI possède une faille de conception et qu'il faut la changer ?

g. Pourquoi autant de sites sont touchés et peut-on craindre une épidémie ?

h. Quel est la parade à ce type d'attaque ?
Quel est le correctif choisi par Microsoft ?
Comment être sûr que cette parade sera également utilisée rapidement par les outils non Microsoft ?

i. Quelles recommandations donneriez-vous aux utilisateurs pour éviter ce problème et que feriez vous, vous-même, en utilisant OpenSSL ?

j. Le journaliste parle de « *phishing* », expliquez ce que c'est et comment cette attaque est mise en œuvre concrètement du point de vue organisation réseau.

2 – Que vous évoque la figure 1 donnée en page 2 si l'opération E est le chiffrement DES ?
2pts Quelle est la relation entre P_n et C_n ?
Écrire la commande OpenSSL correspondante.

3 – Qu'est-ce qu'un MAC et quelles sont les différences avec une signature ?
2pts Est-ce utilisable pour assurer l'authentification d'un document du point de vu juridique ?

4 – Qu'est-ce que le « rejeu » ?
2pts Donnez un moyen utilisé en pratique pour l'éviter.

5 – Dans le cadre d'un concours organisé par Internet, pour gagner la nouvelle tablette « multi-
2pts touche » du constructeur DSKos, sous Android v4.0, « PainSec », les participants doivent répondre à un questionnaire et envoyer leurs réponses par courrier électronique à l'adresse du cabinet d'huissier donné dans le questionnaire.
Pour déterminer le gagnant parmi les participants ayant fourni des réponses correctes au questionnaire, l'huissier choisira le courrier arrivé en premier.
Indiquez comment garantir l'équité de traitement des participants ?

6 – Un télé-travailleur voudrait pouvoir imprimer, depuis chez lui, sur une imprimante située dans
2pts le réseau local de son entreprise, ce réseau étant accessible depuis Internet par un routeur.
Indiquez ce qu'il est possible de déployer comme outil pour fournir une solution sécurisée.