48:69:6D:82:56:56:FA:F4:8E:85:C6:4D:02:95:9B:65 ou le nouveau certificat de notre Autorité de Certification

Martin.Ouwehand@epfl.ch, SIC

Résumé des épisodes précédents

Les systèmes cryptographiques à clef publique permettent principalement deux choses. D'une part, la communication sûre (chiffrée) de données avec un correspondant sans échange préalable d'une quelconque clef secrète: j'encrypte le message avec sa clef publique et la sûreté du système est assurée parce qu'il est le seul à pouvoir le déchiffrer avec sa clef privée, qu'il ne divulgue pas. D'autre part, la possibilité de signer des documents: j'encrypte le document avec ma clef privée et chacun, en le décryptant avec ma clef publique, peut s'assurer que j'en suis l'auteur (je suis le seul à posséder la clef privée correspondante).

Ce merveilleux système a toutefois un point faible: au moment où les correspondants échangent leurs clefs publiques, un scélérat contrôlant le réseau par lequel elles transitent peut les intercepter et les remplacer par des clefs dont il possède les clefs privées correspondantes: il peut alors décrypter tous les échanges entre ces deux malheureuses personnes ou se faire passer pour l'une aux yeux de l'autre (par falsification de signature).

Ce défaut peut se corriger si je recoure à une Autorité de Certification: celle-ci signe (comme indiqué ci-dessus, avec sa clef privée) un document incluant ma clef publique et mon identité (qu'elle doit bien sûr vérifier, c'est même là sa tâche essentielle). C'est le document ainsi signé qu'on appelle **certificat**. Ensuite de quoi, s'il veut encrypter un message qu'il va m'envoyer, mon correspondant n'utilisera ma clef publique qu'en l'extrayant d'un certificat portant mon nom et après avoir vérifié qu'il est correctement signé par l'Autorité de Certification. Pour cette vérification il utilise le certificat de l'Autorité de Certification, un document constitué de la clef publique de celle-ci et d'un identificateur (par exemple *EPFL Certification Authority*), le tout signé par sa clef privée. On dit donc que ce certificat est auto-signé (*self-signed* ou *self-issued* en jargon anglo-informatique).

L'EPFL est dotée d'une telle Autorité de Certification depuis 1998. Les trois premières années de son existence furent assez discrètes, consacrées surtout à l'émission de certificats pour des serveurs Web et à des tests internes au SIC, mais depuis l'année passée le service est accessible à tous les membres de l'Ecole, à travers Gaspar.

Pour plus de détails, voir:

- *http://sawww.epfl.ch/SIC/SA/publications/FI95/fi-7-95/7-95-page3.html*
- *http://sawww.epfl.ch/SIC/SA/publications/FI97/fi-10-97/10-97-page4.html*
- *http://sawww.epfl.ch/SIC/SA/publications/FI01/fi-5-1/5-1-page1.html*

Le Web, principal consommateur de certificats

Les certificats sont utilisés sur le Web quand on doit établir une connexion encryptée avec un serveur et qu'on utilise SSL (Secure Socket Layer) ou son successeur TLS (Transport Layer Security, défini dans le RFC 2246, *ftp://sunsite.cnlab-switch.ch/doc/standard/rfc/22xx/2246*) pour accéder à une URL avec le format *https://gaspar.epfl.ch* (noter le **s** de sécurité après le **http**). Le certificat du serveur est alors utilisé pour l'encryption de cette connexion.

Inversement, un serveur Web peut identifier un visiteur qui lui présente un certificat et lui octroyer alors l'accès à une page confidentielle ou lui permettre d'exécuter un script avec plus de privilèges. Par exemple, les veinards munis d'un certificat signé par l'Autorité de Certification de l'EPFL ont le droit d'accéder sans mot de passe à Gaspar, qui peut connaître leur identité en consultant le nom figurant dans le certificat présenté.

Enfin, les navigateurs octroient plus de privilèges à un applet Java signé à l'aide d'un certificat - non pas, comme on le croit souvent, parce que c'est une garantie qu'il ne fera rien de méchant, comme effacer tous vos fichiers, mais parce que, selon les concepteurs de ce système, le programmeur n'osera rien faire de tel s'il sait qu'il pourra être identifié par la signature électronique effectuée grâce à son certificat.

Hors du Web, mentionnons encore parmi les applications possibles des certificats l'échange de courrier électronique signé ou encrypté, tel que spécifié dans le standard S/MIME (plus de détails sous *http://www.imc.org/smime-pgpmime.html*).

Le certificat, une denrée périssable

Parmi d'autres champs supplémentaires, chaque certificat comporte une date d'échéance après laquelle le certificat ne doit plus être reconnu comme valable. Les cyniques diront que le but de cette durée de validité limitée sert surtout à assurer un revenu aux entreprises émettrices de certificats, mais on offre souvent une autre explication: en obligeant ainsi régulièrement la génération de nouvelles paires de clefs, on décourage les attaques contre la clef privée (sur laquelle est basée la sécurité du système), aussi bien par des moyens cryptographiques (*craquage* de la clef) que par le piratage

informatique (intrusion sur votre PC et subtilisation de votre clef). C'est pourquoi la plupart des certificats personnels émis ont une validité d'une année (c'est le cas à l'EPFL également).

Le nouveau certificat de notre Autorité de Certification

C'est ainsi que le certificat courant de notre Autorité arrive à échéance dans moins d'une année (le 1er février 2003) et que le moment est venu de générer et de publier un nouveau certificat, valable depuis le 23 janvier de cette année jusqu'au 21 janvier 2012. Ce recouvrement d'à peu près une année dans la durée de validité de l'ancien et du nouveau certificat permettra une transition sans heurt dans l'utilisation des certificats dans notre site. Dès le 1er mars 2002, la signature de nouveaux certificats personnels ou de serveur se fera exclusivement avec ce nouveau certificat de l'Autorité de Certification.

Tous les membres de l'EPFL sont donc invités à le charger dans leur navigateur, ce qui se fait en suivant les indications données à cette page: *http://certauth.epfl.ch/CA/cacert.html*.

Explication du titre

Le lecteur attentif aura sans doute remarqué que rien n'empêche le scélérat évoqué au début de l'article de falsifier aussi le certificat de l'Autorité de Certification au moment où mon correspondant va le chercher pour vérifier la signature apposée sur ce qu'il croit être mon certificat. Il est possible de rétorquer qu'il devra alors le faire pour tous les clients de l'Autorité de Certification s'il ne veut pas être découvert et qu'il s'agit donc d'une tâche autrement plus difficile que l'interception et la falsification d'une seule clef publique, mais on voit bien qu'on met là le doigt sur une difficulté de principe incontournable et qu'il vaut mieux assurer par des moyens externes au réseau Internet la possibilité à chacun de vérifier qu'il dispose bien du vrai certificat de notre Autorité de Certification.

La chaîne de caractères hexadécimaux figurant dans le titre de cet article est l'empreinte digitale (*fingerprint* ou *thumbprint* en jargon anglo-informatique) au format MD5 du nouveau certificat de notre Autorité de Certification. L'algorithme de hachage MD5 (décrit dans le RFC 1321, *ftp://sunsite.cnlab-switch.ch/doc/standard/rfc/13xx/1321*) permet d'obtenir un *résumé électronique* de 16 octets (l'empreinte digitale) de n'importe quel document avec la garantie qu'il est impossible de le modifier sans que son empreinte digitale ne change. C'est donc un moyen pratique de vérifier l'intégrité dudit document, surtout si celui-ci est volumineux.

Voici donc comment vérifier au moment du chargement que notre scélérat n'a pas réussi à falsifier le certificat que vous allez chercher. Pour Netscape, lorsqu'apparaît une fenêtre offrant un bouton **More info...**, cliquer dessus: la dernière ligne, intitulée **Certificate Fingerprint**, de la fenêtre apparaissant alors doit contenir la chaîne de caractère mentionnée dans le titre de cet article. Pour Internet Explorer, la fenêtre importante a pour titre **Do you want to ADD the following certificate to the Root Store ?** et la ligne à vérifier est de nouveau la dernière, intitulée **Thumbprint (md5)**.

Il est possible d'effectuer cette vérification à tout moment, et pas seulement au chargement du certificat. Pour Netscape, suivre le chemin **Security → Certificates → Signers**, sélectionner la ligne correspondant à notre Autorité et cliquer sur **Edit**. L'empreinte digitale à vérifier se trouve à la ligne **Certificate Fingerprint** de la fenêtre apparaissant alors. Pour Internet Explorer, sélectionner notre Autorité au bout du chemin **Tools → InternetOptions... → Content → Certificates → Trusted Root Certification Authorities**, cliquer sur **View**, choisir l'onglet **Details** et consulter le champ **Thumbrint**. Surprise, la suite de caractères indiquée ne correspond pas ! L'explication en est qu'Internet Explorer utilise à cet endroit l'algorithme SHA1 (c'est un standard américain, voir *http://www.itl.nist.gov/fipspubs/fip180-1.htm*) au lieu de MD5 et qu'il faut donc vérifier la correspondance avec cette chaîne-ci:

517AE59D 16D6E8F6 4A71359B DE9081A7 B547398E

Cette chaîne apparaît aussi sous la ligne intitulée **Thumbprint (sha1)** lors du chargement initial du certificat.

Si vous pouvez donc vérifier ces empreintes digitales par rapport à une version de cet article dans un exemplaire imprimé du Flash Informatique, vous avez une très grande probabilité d'avoir une copie du vrai certificat de l'Autorité de Certification: nous croyons que les scélérats n'iront pas jusqu'à imprimer des faux Flash Informatique pour vous tromper!

Et les autres Autorités de Certification ?

Pour la plupart des utilisateurs, il n'y a que le certificat de l'Autorité de Certification de l'EPFL qu'ils doivent charger explicitement dans leur navigateur, alors que les certificats des autres Autorités de Certification le sont déjà à l'installation. Ceci fait penser à certains que le certificat de notre Autorité doit donc être moins sûr, que ses bits ne sont pas aussi bien sertis, que son eau est moins éclatante que celle des certificats des autres Autorités de Certification. Ce n'est pas le cas. Le chargement d'un certificat d'Autorité de Certification dans votre navigateur exprime la confiance que vous avez dans le sérieux avec lequel cette Autorité fait sont travail, qui est de garantir l'identité des personnes à qui elle fournit un certificat. En pré-chargeant les certificats de toutes ces Autorités de Certification dans votre navigateur, son fournisseur prend cette décision à votre place (peut-être influencé par quelques poignées de dollars). Il ne semble pas que ce soit toujours une bonne décision, puisqu'une Autorité de Certification dont les certificats sont pré-chargés dans Netscape et Internet Explorer a, dans un incident précis, failli à sa tâche de contrôle d'identité (voir à ce sujet: *http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO59099,00.html*). ■