Attaque réussie contre la signature électronique

- Informatique - Sécurité Informatique -

Date de mise en ligne : jeudi 16 juin 2005

Deux chercheurs sont parvenus à modifier le contenu d'un document signé électroniquement sans altérer la validité de sa signature. Une telle attaque était considérée jusqu'à présent comme purement académique parce qu'il était impossible de contrôler le contenu du document modifié. Les deux chercheurs, eux, peuvent faire signer n'importe quoi et produire n'importe quel autre document... portant la même signature !

Prenez un document électronique. Signez-le. Il est censé ne plus être modifiable : la clé privée qui a certifié la signature prouve l'identité du signataire tandis que l'empreinte du document, fournie par des algorithmes tels MD5 ou SHA-1, est irrémédiablement liée à son contenu. C'est d'ailleurs là tout l'intérêt de la signature électronique par rapport à son équivalent sur le papier : elle certifie aussi que le contenu du document n'a pas été modifié depuis sa signature.

Mais cela pourrait bientôt ne plus être tout à fait le cas. Lors de la dernière conférence Eurocrypt 2005, deux chercheurs allemands ont présentés une attaque particulièrement sournoise contre les signatures électroniques générées grâce à l'algorithme MD5. Ils sont parvenus à faire signer un document et à présenter ensuite un autre, totalement différent, portant la même signature... qui était toujours valide ! Pour le petit monde des passionnés de cryptographie, cela tient de la magie. Mais pour celui de la sécurité informatique, c'est surtout une nouvelle inquiétante.

Pour parvenir à leur fin, les deux chercheurs ont mis en oeuvre conjointement une obscure caractéristique propre aux documents Postscript et une attaque mathématique connue contre l'algorithme MD5. La première phase de l'attaque consiste à glisser deux documents totalement différents au sein du même fichier Postscript. Un seul de ces documents peut-être visible à la fois tandis que l'autre demeure caché dans le fichier. La bascule entre les deux versions se fait en changeant simplement le nom interne des documents au sein du fichier Postscript. Nous sommes pour l'instant encore loin de l'attaque high-tech, mais cela va venir. Car chaque version du contenu se voit attribuer un nom interne (un label) calculé en utilisant une attaque déjà connue contre MD5, dite "de collision". Cette attaque permet de créer des contenus différents qui généreront pourtant la même signature (le même hash) MD5. Jusqu'à présent cette attaque était considérée comme purement académique car il est impossible de créer des contenus qui "veulent dire quelque chose". Oui mais voilà : en utilisant cette technique pour créer deux noms différents à la signature identique, peu importe qu'ils ne veulent rien dire : ils ne sont destinés qu'à spécifier au sein du document quelle version doit être affichée. Grâce à cela, les deux chercheurs peuvent ensuite échanger à loisir les labels au sein du document signé sans que la signature n'en soit affectée, et donc rendre visible la version illégitime du contenu.

Le scénario d'attaque impliquerait donc de réaliser à l'avance un fichier Postscript contenant un premier document -visible- totalement anodin et un second, caché, qui contient le texte à faire signer illégalement. Une fois le texte anodin signé, il suffit alors d'éditer le fichier Postscript pour remplacer le label du document anodin par celui de la version cachée. Puisque les deux produisent la même signature MD5, le fichier Postscript lui-même demeure totalement inchangé aux yeux de l'algorithme. Et sa signature est donc toujours valide.

Bien sûr, cette attaque ne concerne pour l'instant que des documents Postscript signés avec l'algorithme MD5. C'est plutôt limité, et il ne s'agit bien que d'une attaque, et non d'une nouvelle vulnérabilité des algorithmes de signature. Mais du côté des spécialistes on s'attend à voir apparaître des variantes capables de fonctionner avec l'algorithme SHA-1 (pour lequel des attaques de collision existent déjà) et d'autres formats de documents avancés capables de gérer le support de plusieurs versions d'un même contenu. Voilà de quoi faire de la publicité pour un format simple tel que le XML...

En attendant les parades éventuelles, si vous devez signer un document électronique, jetez-y un oeil avec un éditeur de texte avant d'aposer votre signature !