Medienbeobachtung AG

L'AGEFI
13.01.2010 Seite 1 / 1
Auflage/ Seite 10000 / 4 1772
Ausgaben 250 / J. 7647125

Le décryptage de clés de sécurité fait sauter les limites

L'accès protégé à des sites internet n'est plus garanti selon un consortium de chercheurs. Dont une équipe de l'EPFL.

JÉRÉMY NIECKOWSKI

Des chercheurs ont mis en commun leurs capacités de calcul et sont parvenus à «casser» une clé de sécurité, appelée encore clé RSA (cryptographie à clé publique). Dans les faits, cette équipe internationale de scientifiques (de l'EPFL, l'INRIA (France), NTT (Japon), l'Université de Bonn (Allemagne) et CWI (Pays-Bas)) a mis deux années et demie pour accéder aux informations contenues dans une clé RSA de 768 bits, en extrayant les facteurs premiers de ses 232 chiffres grâce notamment à la puissance de traitement des processeurs modernes.

¨Si les standards utilisés actuellement sont au dessus de ceux choisis dans cette étude, précisent les scientifiques, cette prouesse technique soulève quelques questions notamment sur la capacité des fournisseurs d'accès à des informations en ligne (banques, site d'achats, organismes d'Etats ou centrale médicale, entre autres) à garantir la sécurisation des informations contenues sur des cartes à puces ou circulant sur ces sites. Les systèmes cryptographiques sont en effet censés garantir la sécurité des échanges de données sur Internet et ils sont par exemple au cœur du commerce électronique, que ce soit sur les sites «http» ou «https». S'assurer de leur fiabilité est crucial à un moment où les barrières de sécurité tombent.

PAOLO BUZZI (Swissquote). Avec le certificat, c'est le contenu des informations d'un site qui est aussi visé par les attaques.

L'ensemble des interlocuteurs contactés par *L'Agefi* saluent le succès de cette opération. Mais tous soutiennent que cela ne représente pas un danger direct pour le client ou visiteur d'un site internet. Les banques ou plateformes de trading en ligne utilisent actuellement des certificats avec des clefs RSA à 1024 bits (soit une solution mille fois plus évoluée que celle de 728 bits). D'ici 2012, la norme devrait être à 2048 bits. «Les scientifiques ont réussi à décrypter un accès qui chez nous intervient au moment où l'investisseur tape l'Url pour accéder à la partie appelée banking. Soit avant même le moment où les clients devraient inscrire leurs codes personnels pour accéder à leurs comptes. Une fois la connexion établie, d'autres procédés de cryptages interviennent. Les clients ne doivent donc pas avoir peur de voir leurs comptes piratés. Si une attaque devait être menée ce serait sur notre site, pas sur les comptes des clients», explique Paolo Buzzi, directeur technique chez Swissquote. La situation n'est donc pas à risque aujourd'hui clament les interlocuteurs. «Seule l'opération qui consiste à l'échange initial des clefs pour accéder à un site internet https pourrait potentiellement être concernée par cette tentative de décryptage, au moment où une personne tente d'accéder à un site et pas au moment où celle-ci tente d'accéder à ses informations personnelles», ajoute-t-il.

Reste que même si les chercheurs ont mis plusieurs années à parvenir à leur fin, il parait d'autant plus judicieux «d'utiliser de plus hauts niveaux de sécurité que ceux offerts par la clé RSA de 1024 bits dans cette période de transition», insiste Arjen Lenstra, du Laboratoire de cryptologie algorithmique à l'EPFL. L'étude a révélé en effet qu'aucun système n'est sûr à 100%. «En fait, parvenir au décryptage des données protégées par les protocoles SSL (ou autre d'ailleurs) n'est qu'une question de temps à disposition et de puissance de calcul. L'approche et les mesures de sécurité en place sont toujours basées sur une protection qui empêche un accès aux données ou informations dans un délai utilisable (plusieurs centaines d'années) avec les puissances de calcul les plus importantes», explique Paul Coudret, conseiller économique de la BCV.

L'heure est donc à la sérénité du côté des établissements bancaires ou financiers. «Avec les autres banques et d'autres partenaires publics ou privés, nous travaillons sans cesse pour améliorer les conditions de sécurité. Le client lambda n'a donc aucune raison d'avoir peur de voir ses codes d'accès crackés à l'heure actuelle par des clés cassés», conclut Marc Andrey, porte parole de PostFinance, le numéro un suisse du ebanking (avec 1,1 millions d'utilisateurs).

LA SITUATION N'EST DONC PAS À RISQUE AUJOURD'HUI CLAMENT LES SPÉCIALISTES INFORMATIQUES.