Le chiffrement exposé à des portes dérobées

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 23 novembre 2007

Deux experts de la cryptologie ont récemment donné de la voix. Des bugs dans les microprocesseurs et une faille dans un générateur de nombres aléatoires pourraient cacher des portes dérobées.

Deux experts de la cryptologie, étymologiquement la science du secret, ont tiré la sonnette d'alarme pour mettre en garde les entreprises. Le premier et pas des moindres puisqu'il est l'un des créateurs du fameux algorithme RSA, Adi Shamir, a publié une note sur les risques encourus par le chiffrement du fait de l'existence de bugs dans les microprocesseurs.

D'après les travaux du chercheur israélien, ces erreurs de conception pourraient en effet rendre vulnérables des procédés de chiffrement. Pour le responsable scientifique et directeur des laboratoires RSA, Ari Juels, la démonstration de son confrère "ne décrit pas une attaque sur l'algorithme à proprement parler. Elle décrit une technique pour un attaquant permettant de contourner les opérations de l'algorithme de RSA au moyen d'une porte dérobée dans le microprocesseur sur lequel il est exécuté. Aucune backdoor de cette nature n'est pour l'instant connue".

Deux experts de la cryptologie, étymologiquement la science du secret, ont tiré la sonnette d'alarme pour mettre en garde les entreprises. Le premier et pas des moindres puisqu'il est l'un des créateurs du fameux algorithme RSA, Adi Shamir, a publié une note sur les risques encourus par le chiffrement du fait de l'existence de bugs dans les microprocesseurs.

D'après les travaux du chercheur israélien, ces erreurs de conception pourraient en effet rendre vulnérables des procédés de chiffrement. Pour le responsable scientifique et directeur des laboratoires RSA, Ari Juels, la démonstration de son confrère "ne décrit pas une attaque sur l'algorithme à proprement parler. Elle décrit une technique pour un attaquant permettant de contourner les opérations de l'algorithme de RSA au moyen d'une porte dérobée dans le microprocesseur sur lequel il est exécuté. Aucune backdoor de cette nature n'est pour l'instant connue".

Des contremesure permettent de se prémunir contre les bugs des processeurs

Pour autant, des parades logicielles existent au procédé d'attaque décrit par Adi Shamir. Il en est effet possible de mettre en oeuvre des mécanismes de vérification des calculs cryptographiques réalisés. De semblables contremesures sont déjà appliquées aux cartes à puces, elles aussi sujettes à attaques via la génération d'erreurs au niveau de la puce.

RSA, grâce à BSAFE dispose d'ailleurs d'outils permettant d'appliquer ces contremesures aux implémentations de son algorithme. OpenPGP, qui exploite également l'algorithme RSA comprend aussi ces mécanismes défensifs apportant la possibilité de se prémunir contre la vulnérabilité décrite par le professeur Shamir.

Cependant cette sécurisation supplémentaire n'est pas neutre puisqu'elle a notamment pour contrainte d'accroître significativement la durée d'exécution de l'algorithme sur les ordinateurs. Le processus de vérification peut ainsi à lui seul exiger autant de temps que le chiffrement du message lui-même.

Quant à une possible exploitation de la vulnérabilité par des agences gouvernementales, le contexte sécuritaire

mondial et la lutte contre le terrorisme en font une hypothèse crédible, mais difficilement vérifiable. Pour Bruce Schneier, cryptanaliste de renom et dirigeant de la société de sécurité BT Counterpane, le recours à une backdoor dans un générateur de nombres aléatoires est au moins évident.

La NSA à l'origine d'une méthode de chiffrement vulnérable

Le NIST, dont le but est de développer des standards de sécurité pour les agences fédérales, servant souvent ensuite de recommandations aux agences non gouvernementales et aux entreprises, a approuvé quatre méthodes de nombres aléatoires déterministes. Bruce Schneier est ainsi revenu sur les faiblesses révélées par les cryptanalistes sur l'une d'entre elles basée sur une courbe elliptique.

En plus d'une faille de conception, cette méthode standardisée par le NIST et poussée par la NSA (l'agence américaine spécialisée dans la surveillance des communications) comporte une deuxième faiblesse bien plus grave s'apparentant pour Bruce Schneier à une porte dérobée.

"Elle est basée sur des constantes dont la connaissance permet de prévoir les prochains nombres générés. De façon concrète, en appliquant au protocole TLS, cela suppose que la connaissance d'une seule transaction TLS permettrait de casser ensuite toutes celles émises par le même ordinateur", détaille le consultant de Solucom.

L'existence de ces constantes et leur possible possession par un tiers rendent toute opération de chiffrement basée sur ce générateur de nombres aléatoires vulnérables à qui les possèdent.

Pour Bruce Schneier, il est donc tout à fait légitime de s'interroger sur le caractère fortuit de cette faiblesse négligée par la NSA. L'agence et le NIST devront certainement apporter des explications.

Post-scriptum :

http://www.journaldunet.com/solutio...