Casser un chiffrement PGP en utilisant le cloud d'Amazon

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 9 novembre 2009

Les machines virtuelles d'un nuage informatique aident à réduire l'effort de cryptanalyse, comme le montre l'expérience d'un cabinet de conseil américain.

Pour les hackers aussi, le cloud computing ouvre de nouvelles perspectives intéressantes, comme le montre le cabinet de conseil en sécurité Electric Alchemy. A la demande d'un client, cette société américaine a voulu trouver le mot de passe d'un fichier ZIP chiffré en PGP (Pretty Good Privacy). Elle a donc installé, sur un PC Windows 7 à double coeur, le logiciel Distributed Password Recovery de l'éditeur russe Elcomsoft, qui permet de trouver des mots de passe par attaque en force brute (c'est-à-dire en testant toutes les combinaisons possibles).

D'abord, ce fût la déception : le logiciel a indiqué un délai de 2 100 jours pour casser le chiffrement, soit plus de cinq ans. Electric Alchemy a donc commencé à déployer des instances Elcomsoft sur Amazon Web Services. Avec une dizaine de machines virtuelles en option high CPU, le délai s'est retrouvé ainsi réduit à 122 jours. Avec un tarif horaire de 30 cents par instance virtuelle, le coût total de l'attaque est, dans ce cas, de 8 784 dollars.

Dix millions de dollars pour casser 10 caractères

Mais pas de panique, il ne s'agit là que d'un exemple. Cette attaque s'est révélée relativement peu onéreuse car le mot de passe en question était simple. Le cabinet a réitéré toute une série d'attaques par force brute sur différents types de mot de passe. Conclusion : même en utilisant Amazon Web Services, il faudrait dépenser 10 millions de dollars pour casser un mot de passe d'une longueur de 10 caractères ASCII.

Post-scriptum :

http://pro.01net.com/editorial/5081...