Les secrets de Skype rendus publics ?

- Informatique - Software -

Date de mise en ligne : jeudi 15 juillet 2010

Spyworld Actu

Des experts en cryptographie ont diffusé sur internet des fichiers permettant de mieux comprendre les protocoles de cette application. Une grosse pierre dans le jardin secret de Skype.

Les pirates vont-ils s'engouffrer dans Skype grâce aux travaux menés par l'équipe de Sean O'Neil ? Connu pour avoir créé l'algorithme de hachage EnRUPT, ce cryptographe a en effet publié sur son site trois fichiers, dont deux codes sources. Ces éléments permettent de comprendre un peu mieux les rouages de Skype. Sean O'Neil affirme sur son site qu'il est « possible d'accéder (et donc de modifier) un grand nombre d'informations dans le trafic. Vous aussi pouvez décrypter et analyser toute connexion et vous pouvez développer des applications interopérables permettant de dialoguer avec les serveurs de Skype et les supernoeuds (regroupement d'utilisateurs, NDLR) ».

Il faut néanmoins relativiser cette annonce. Elle ne remet pas en cause la confidentialité des données transitant par ce réseau. Certes, le code publié (générateur de clef RC4) est la pierre angulaire du système de camouflage du trafic Skype mais il ne suffit pas, à lui seul, à observer les rouages internes de ce réseau P2P. D'autant que la société Skype a déjà prouvé qu'elle pouvait mettre à jour son protocole.

Pas de risques pour les entreprises ?

Sean O'Neil se montre d'ailleurs rassurant : « la publication de ces éléments permet aux entreprises et aux éditeurs de logiciels de sécurité d'ajouter la capacité de scanner le trafic de Skype afin de combattre l'exploitation de vulnérabilités ». Les techniques qu'il a employées sont encore floues car les protections de Skype sont nombreuses. « Il existe sept types de cryptage de la communication » précise O'Neil qui a prévu de tout expliquer en décembre lors du prochain rendez-vous du Chaos Communication Congress à Berlin. « L'objectif est le développement d'un client Skype en logiciel libre. Pour cela, il faut pouvoir ré-implémenter le chiffrement utilisé par cette application. Or, Skype a réalisé des modifications afin de ne pas utiliser un système standard mais demeurer complètement propriétaire. Cet aspect propriétaire est en train de tomber », explique Hervé Schauer du cabinet spécialisé en sécurité informatique HSC.

Ce n'est pas la première fois que des experts en sécurité s'attaquent à la forteresse Skype. Lors des conférences Black Hat Europe et SSTIC 2006, deux experts du Centre de recherche d'EADS, Philippe Biondi et Fabrice Desclaux, avaient présenté les résultats de leur analyse.

Post-scriptum :

http://pro.01net.com/www.01net.com/...