

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article12560>

Quand la cryptographie donne à la parole valeur de contrat

- Technologie -



Date de mise en ligne : jeudi 28 janvier 2010

Spyworld Actu

Le Fraunhofer a mis au point une signature numérique qui permet à un accord oral de tenir lieu de signature : elle transforme les échanges téléphoniques en une chaîne cryptographique incassable.

Au lieu de se déplacer pour signer leur contrat, les professionnels pourraient tout simplement sceller leur accord au téléphone. C'est en tout cas ce que préconise un groupe de chercheurs allemands, de l'[Institut Fraunhofer SIT](#) (pour Secure Information Technology) : ils ont mis au point un système de signature numérique qui permet de transformer une communication téléphonique en engagement légal à valeur de contrat. Celui-ci fonctionne pour les communications en VoIP, autrement dit les échanges téléphoniques s'effectuant via Internet ou tout autre réseau acceptant le protocole TCP/IP. Le dispositif de signature repose sur la cryptographie pour assurer un niveau élevé de sécurité.

Sécuriser les échanges téléphoniques

Une empreinte cryptographique vient marquer chaque intervalle présent dans la conversation téléphonique, ce qui protège l'ordre et la cohérence de la communication", explique à L'Atelier Rachid El Khayari, l'un des scientifiques impliqués dans ce projet. En clair, lorsque les deux interlocuteurs décident de conclure un accord, ou de signer un contrat, il leur suffit d'enclencher l'enregistrement de la conversation. Le système transforme celle-ci en une chaîne cryptographique qu'il est impossible de modifier par la suite, sans laisser de traces. La conversation téléphonique est en effet "signée". Et ce de manière continue, tout au long du processus d'enregistrement.

Toute modification brise la "signature" téléphonique

Cela signifie que si quelqu'un tente de manipuler l'archive téléphonique (qu'il s'agisse de couper certaines parties de la conversation, ou d'intégrer d'autres parties à tel ou tel moment de la séquence) la signature enregistrée préalablement se brise, et devient inutilisable. A noter : le système peut être installé sur n'importe quel appareil qui permet d'établir des connections VoIP. Cela comprend donc un certain nombre de téléphones mobiles. Il sera présenté à l'occasion du Mobile World Congress, qui se tiendra à Barcelone du 15 au 18 février.

Post-scriptum :

<http://www.atelier.fr/applications/...>