

Vuvuzela, une messagerie qui cache les métadonnées



Vuvuzela est une nouvelle messagerie qui prétend qu'elle peut cacher les métadonnées. Le concept est encore très expérimental, mais il est assez prometteur.



Vuvuzela est un concept de messagerie qui permet de communiquer en cachant les métadonnées. Elle est développée par David Lazar, un doctorant du MIT qui travaille sur le chiffrement et les systèmes distribués. Il a publié un papier qui décrit les principes de Vuvuzela.

Des protocoles comme TOR permettent d'avoir un certain anonymat, mais il reste vulnérable à une analyse du trafic. Avec Vuvuzela, la messagerie est spécialement conçue pour se protéger contre la surveillance gouvernementale sur les métadonnées. La NSA a admis à plusieurs reprises qu'il ne sert à rien de chiffrer les données si les métadonnées sont en clair.

Les métadonnées englobent de nombreuses informations, mais on peut les résumer par le fait qu'elles pointent vers l'identité d'une personne et les contacts de cette personne. Vuvuzela veut cacher les métadonnées, mais elle ne peut pas cacher 2 métadonnées. La première est le nombre d'utilisateurs connectés sans une conversation et la seconde concerne les utilisateurs actifs dans une conversation. Mais Vuvuzela réduit également ce problème en ajoutant des nuisances aux métadonnées.

Le concept est intéressant, mais il n'est pas prêt pour le déploiement. On peut suivre le projet sur Github.



Réagissez à cet article

Source

<http://actualite.housseniawriting.com/technologie/2015/12/04/vuvuzela-une-messagerie-qui-cache-les-metadonnees/11327/>