

Google part en guerre contre les faux certificats SSL

Google veut se prémunir des risques de sécurité lié aux certificats SSL dont l'usurpation peut tromper l'utilisateur qui s'est pourtant assuré de l'authenticité du site qu'il visite grâce à ce « passeport numérique ». En témoigne l'affaire Comodo, nom du fournisseur américain de certificats numériques, [qui s'est fait dérober 9 certificats SSL](#) pour les domaines touchant Microsoft, Google, Yahoo, Mozilla ou encore Skype. La firme de Mountain View a donc décidé de renforcer l'intégrité de ses certificats SSL (Secure Sockets Layer).

Sur le blog [Google Online Security](#), Ben Laurie, ingénieur en chef chez Google, dévoile deux nouveaux projets destinés notamment à éviter de futurs incidents concernant la gestion de ses certificats numériques, nous apprend [l'Espresso.fr](#). Google compte ainsi établir un catalogue en ligne pour les certificats SSL. Ben Laurie explique que la firme de Mountain View va utiliser son logiciel d'exploration Web pour examiner des sites et recueillir un certain nombre d'informations sur leurs certificats de sécurité.

Google prévoit ensuite d'intégrer ces informations au Google Certificate Catalog, une base de données des certificats SSL pour les connexions, permettant de vérifier l'authenticité des données des certificats numériques. Il compte également collaborer avec le groupe de travail DNS-based Authentication of Names Entries (DANE), qui élabore une plate-forme permettant de spécifier et de valider la signature des certificats SSL.