Des 'hackers' créent de faux certificats de sites sécurisés

La petite image qui s'affiche dans le coin de votre navigateur pour indiquer qu'un site est compromis ou non pourrait jouer de mauvais tours. Voilà les conclusions d'une équipe transnationale de chercheurs en informatique.

Des scientifiques américains et européens viennent de montrer que l'on peut utiliser le **réseau en grid de la PlayStation 3** pour créer de faux certificats. Ils sont parvenus à intégrer ces certificats truqués sur un navigateur, ce dernier considérant alors que la connexion est sécurisée. Edifiant.

Ces scientifiques plutôt hardis du **Centre Wiskunde & Informatica** (CWI) de Californie mais aussi de l'**Université de Technologie des Pays-bas à Eindhoven** et des équipes de l'**Ecole polytechnique de Lausanne** ont parlé de leur découverte lors d'un congrès dédié à la sécurité à Berlin.

Dans la capitale allemande, ils ont montré qu'ils étaient capables de **générer deux messages différents avec une seule signature électronique**. Pour cela ils ont utilisé un algorithme de leur composition.

Les chercheurs ont donc montré qu'il ne fallait **pas avoir une confiance aveugle dans les sites dont les URL débutent par https** puisqu'ils sont maintenant « piratables », certes par des mains expertes. L'intérêt de la méthode réside alors dans le fait que le navigateur est leurré: il considère qu'il s'agit bel et bien d'un site valide et correctement identifié. D'autant que le **certificat digital MD5** est toujours utilisé par de nombreux sites même s'il permet d'être activé par des tiers pour créer de faux certificats de validité.

Cette vulnérabilité aurait déjà été identifiée voilà quatre années par des **chercheurs chinois** qui avaient noté ce phénomène lorsqu'ils ont fait s'affronter deux signatures digitales identiques. L'une valide, l'autre pirate.

Cette technologie de *hacking*n'en est qu'à ses balbutiements puisque la puissance nécessaire pour effectuer ce type d'attaque nécessiterait **30 années de calcul pour un ordinateur traditionnel.**

Or

, l'utilisation du « réseau » de la PlayStation 3 a réduit ce délai à**trois jours seulement.** De quoi inquiéter les éditeurs de navigateurs Web.

Si cette faille était utilisée massivement le ***phishing*** ou arnaque aux faux sites s'en trouverait d'autant plus facilité. Il serait alors bien plus compliqué de démasquer le faux du vrai.