Résumé - Projet Audit des implantations SSL/TLS

1 Objet

Vous souhaitez savoir comment retrouver les clés privées des certificats de serveurs web sécurisés mis en ligne par des grandes entreprises ? Notre projet consistait à "évaluer" le niveau de sécurité du web.

En effet, le monde de la cryptographie est en proie à de grandes incertitudes suite à des révélations et il remet en question tous les systèmes jusqu'alors développés. Ce ne sont pas les algorithmes des systèmes cryptographiques qui sont remis en cause, mais leur développement machine qui n'est pas (ou plus) considéré comme nécessairement sûr.

Pour répondre à cette problématique, le projet s'est déroulé en trois parties, que nous présenterons vendredi 28 à 14h :

1. Après avoir scanné les ports de serveurs web sécurisés d'internet, nous avons récupéré leurs certificats afin d'en extraire les clefs publiques associées. Nous ensuite tenté de les factoriser et avons pu récupérer certains nombres premiers ayant permis leur génération.
2. Au vu de ces résultats, nous avons essayé de trouver l'origine du problème, en auditant notamment le code d'OpenSSL. Nous avons pu répertorier des failles existantes au niveau de la gestion d'entropie, la génération des clefs, le chiffrement, les signatures et les protocoles SSL/TLS.
3. Enfin, en analysant les protocoles SSL/TLS d'OpenSSL, nous avons mis en place un serveur web sécurisé qui permet de tester le certificat d'un navigateur client.

2 Membres du projet - RandomGuys

— Pascal Edouard, *grand manitou, highcharts master.*
— Claire Smets, *CVE buster.*
— Julien Legras, *SSL master, bad C code eater.*
— Mathieu Latimer, *détracteur de la NSA qui souhaite quand même travailler pour eux, pourvu qu'ils payent bien.*
— William Boisseleau, *l'insaien, au bord du suicide après avoir lu le code d'OpenSSL.*