Université de Rouen

Projet Audit des implantations SSL/TLS

Compte rendu de réunion 1

7 novembre 2013

Présents :
Pascal Edouard, *Chef de projet*
Claire Smets, *Resp. communication*
William Boisseleau, *Rédacteur CR1*
Matthieu Latimier
Julien Legras

Client :
Ayoub Otmani, *Prof. Université de Rouen*

Résumé

Ce rapport résume les différents éléments évoqués durant la première réunion de projet *audit des implantations SSL/TLS*.

1 Contenu abordé

1.1 Contexte du projet

Le projet s'inscrit dans un cadre relatif à un fait d'actualité récemment mis à jour, lié aux révélations de Snowden sur les pratiques de la NSA. Le monde de la cryptographie est en proie à de grandes incertitudes suite à ces révélations et remet en question tous les systèmes jusqu'alors développés. Notons que 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. La NSA a par exemple très bien pu introduire des *backdoors*, ou faiblesses dans les logiciels, de telle sorte qu'ils puissent accéder aux données claires sans difficultés. On peut par exemple remettre en questions les outils développés par des laboratoires tels que RSAlabs, ou même encore des standards proposés par des agences comme le NIST (Openssl, AES, sont-ils vraiment sûrs ?).

Nous allons notamment dans ce projet étudier la générations des clés pour RSA.

1.2 Première étape : Audit des clés cryptographiques

La première partie du projet consiste à faire un état des lieux des certificats RSA sur internet. Pour ce faire, nous allons :

1. récupérer des certificats RSA contenant les clés publiques sur internet.
2. analyser les certificats et les regrouper par famille (*issuer*).
3. effectuer un PGCD sur ces certificats afin de voir s'il y a des entiers premiers partagés.
4. présenter les résultats obtenus sur une interface et les analyser.

Ainsi, on pourra constater si les générateurs de nombres premiers aléatoires sont calibrés correctement. Lorsque ce n'est pas le cas, on pourra conclure :

— soit l'on considère le générateur comme mal implémenté,
— soit l'on considère que ces failles ont été implémentées intentionnellement.

L'objectif est donc de fournir au client un outil dans un langage choisi (à établir) effectuant ces quatre tâches. L'algorithmique de notre programme devra être optimisée (nota. pour le calcul du PGCD), suivant par exemple les éléments développés dans l'article *Mining Your Ps and Qs, Detection of Widespread Weak Keys in Network Devices*.

1.3 Deuxième étape : Analyse statique

Dans une deuxième partie, nous effectuerons un audit d'OpenSSL :

1. Nous étudierons tout d'abord les recommandations et les standards actuels (cf. PKCS) sous forme d'état de l'art, et nous en choisirons de façon argumentée un standard sur lequel nous baserons nos analyses.
2. Nous analyserons dans un deuxième temps le code source d'OpenSSL, en particulier sa partie développant la génération d'éléments aléatoires et ses primitives cryptographiques. Nous en ferons de plus une description détaillée. Nous comparerons ensuite nos résultats avec les recommandations choisies, puis nous conclurons en déterminant si cette génération est efficace.

1.4 Troisième étape : Analyse dynamique

Suivant le temps restant, il nous est proposé d'implémenter un système serveur permettant l'audit des clients. Le logiciel sur le serveur doit évaluer la sécurité du client suivant un protocole établi, en analysant son système et/ou lui proposant des challenges spécifiques, en particulier autour de SSL. Le logiciel devra rendre un diagnostic et un rapport sur les différents éléments analysés, afin de permettre au client de constater des problèmes lorsqu'il y en a, et d'en connaître leur provenance.

2 Travail demandé pour la prochaine réunion

La prochaine réunion avec le client est fixée au **14 novembre 2013, 13h**, dans le bureau du client. Le travail du groupe pour la réunion est d'étudier l'article *Mining Your Ps and Qs, Detection of Widespread Weak Keys in Network Devices* et d'en concevoir un résumé, afin que nous puissions en discuter avec le client. Le groupe commencera également à réfléchir à une STB, et pourra en proposer une ébauche.