

Cahier Des Charges

AYOUB Pierre - BASKEVITCH Claire - BESSAC Tristan -
CAUMES Clément - DELAUNAY Damien - DOUDOUH Yassin

Stéganographie & Stéganalyse

Mercredi 14 Mars 2018

1 Introduction

1.1 Définition des termes du sujet

La stéganographie est l'art de la dissimulation, appliquée en informatique en cachant des données dans d'autres données. Cette dissimulation se fait généralement au sein de fichiers multimédias. La stéganographie se différencie de la cryptographie, qui correspond à chiffrer un message afin qu'il soit illisible par une personne différente de l'émetteur et du destinataire. En effet, un message chiffré en cryptographie sera visible par tous mais illisible, tandis qu'un message caché dans un fichier f en stéganographie ne sera vu que si un inconnu sait que f contient un message et connaît l'algorithme pour l'interpréter.

La stéganalyse, quant à elle, est la recherche de données cachées dans des fichiers suspects. Si ces données sont identifiées, il faut ensuite réussir à les extraire pour les lire.

1.2 Historique

La stéganographie est une méthode très ancienne dont la première référence à cette utilisation date du premier siècle avant Jésus-Christ. Elle apparaît dans un récit écrit par Hérodote qui raconte comment deux citoyens communiquaient secrètement : le premier citoyen rasait la tête de son esclave et lui écrivait un message sur son crâne. Ensuite, il fallait attendre que les cheveux de l'esclave repousse puis envoyer ce dernier chez le deuxième citoyen. Ce dernier devait de nouveau raser la tête de l'esclave pour découvrir le message qui lui était destiné. Une autre utilisation de la stéganographie consistait à utiliser de l'encre invisible à l'oeil nu, mais qui était révélée à la chaleur.

Avec l'émergence de l'Informatique, les techniques de Stéganographie se sont renouvelées. En effet, il est désormais possible de cacher des données dans d'autres données. Cette multiplicité de techniques stéganographiques grâce à l'Informatique montre l'étendue de cette application dans tous les domaines. Par exemple, la stéganographie moderne a été utilisée dans des communications terroristes (transmission de messages) ou dans les signatures de fichiers multimedia (tatouage numérique) afin de protéger les droits d'auteurs.

2 Fondements du projet

Le but du projet est de réaliser un logiciel de Stéganographie. Les utilisateurs ciblés sont des personnes lambda qui veulent communiquer sans que l'on soupçonne que leurs communications sont en réalité compromettantes.

Le but de l'application est de permettre à un utilisateur U_1 d'envoyer des données cachées à un autre utilisateur U_2 . Ce deuxième utilisateur devra pouvoir interpréter ces données en utilisant la même application que U_1 .

2.1 Motivation du projet

La motivation du projet est venue par notre envie de la majorité des membres de ce groupe de projet d'obtenir le master Secrets. En effet, nous voulions tous réaliser un projet en rapport à la cryptographie et c'est donc pour cela que nous nous sommes réunis afin de réaliser ce type de projet.