Analyse et conception de techniques opérationnelles de stéganographie

Nicolas Bodin

Diffusion Restreinte
Spécial France

École Polytechnique

N° attribué par la bibliothèque

THÈSE

pour obtenir le grade de

Docteur de l'École Polytechnique

Spécialité : **Informatique et mathématiques appliquées**

préparée au laboratoire **de Cryptologie et Virologie Opérationnelles**

présentée et soutenue à huis clos par

Nicolas BODIN

le 28 août 2013

Titre:

Analyse et conception de techniques opérationnelles de stéganographie

Directeur de thèse: **Éric Filiol**

Jury

Rapporteurs	M.	Patrick Bas
	M.	Marc Chaumont
	Mme.	Caroline Fontaine
Examinateurs	M.	Johann Barbier
	M.	Christophe Guyeux
	M.	Jean-Marc Steyaert

Analyse et conception de techniques opérationnelles de stéganographie

Résumé

La stéganographie est la science de l'écriture cachée. Dans ce contexte, un individu tente de communiquer avec une entité sans éveiller les soupçons sur le fondement même de la communication. Cette science vient en complément de la cryptographie (sécurisation de la communication – COMSEC) lorsqu'un besoin d'invisibilité de la communication se fait sentir. Cette thèse, réalisée sous la tutelle et au profit de l'État Major des Armées, traite donc des différentes techniques permettant l'élaboration d'un schéma de stéganographie (sécurisation de la transmission – TRANSEC), techniquement opérationnel et assez solide, visant à insérer un message d'une dizaine de kilo-octets dans une image JPEG de dimensions raisonnables, et capable de résister aux différentes attaques données par l'état de l'art. Afin de rendre ce schéma le plus sûr possible, les formats de données les plus courants sont étudiés (JPEG, BMP, MP3), avant de définir un premier algorithme d'insertion. Ce dernier, fondé sur les travaux de Hopper, reste conceptuel mais permet de définir les fondements de notre algorithme (nommé IMEI). Ce dernier maximise l'efficacité d'insertion, et donc minimise le nombre de modifications apportées au cover-médium. Une analyse de l'algorithme HUGO présenté dans le contexte du challenge BOSS va nous permettre de définir un protocole de stéganalyse, ainsi qu'une deuxième brique importante pour l'IMEI. La dernière partie de ce manuscrit regroupe la partie stéganalyse, avec l'évaluation de l'IMEI et une stéganalyse réellement opérationnelle dans laquelle nous pouvons retrouver une étude de l'utilisation concrète de la stéganographie et de son évaluation.

Mot-clefs : stéganographie, stéganalyse, opérationnel, TRANSEC, Hopper

Abstract

Steganography is the science of writing hidden messages. In this context, an individual attempts to communicate with an entity without arousing suspicious on the very existence of this communication. This science completes cryptography science (COMmunication SECurity – COMSEC) when invisibility in addition to security is required. This PhD work, which has been carried out under the guidance and on behalf of the French military headquaters (EMA) deals with different methods allowing the design of a steganography scheme (TRANSmission SECurity – TRANSEC), technically operational and strong enough to insert a message of approximately ten kilobytes in a JPEG picture of reasonable dimensions, and capable of resisting against attacks given by the state of the art. To make this scheme as safe as possible, the most common data formats are studied (JPEG, BMP, MP3) before defining a first insertion algorithm. This algorithm, based on Hopper's works, is still a proof of concept but allows to define the basis of our new algorithm (named IMEI). The latter maximizes embedding efficiency, and so on, minimizing number of changes applied to the cover-medium. An analysis of HUGO algorithm presented in the context of BOSS challenge gives us the oppportunity to define a steganalysis protocol as well as a second basis for IMEI. The last part of this thesis deals with steganalysis including both IMEI security evaluation, and an operational steganalysis in which we can find a study of a real-life use of steganography and its evaluation.

Keywords : steganography, steganalysis, operational, TRANSEC, Hopper