Transformation de programme et protection de la propriété intellectuelle - préparation, intégration et vérification

Christophe Grenier

École Polytechnique

N° attribué par la bibliothèque

THÈSE

pour obtenir le grade de
Docteur de l'École Polytechnique
Spécialité : **Sécurité Informatique**
préparée au laboratoire **de Cryptologie et Virologie Opérationnelles**
dans le cadre de l'École Doctorale **EDX 447**
présentée et soutenue à huis clos
par

Christophe GRENIER

le 2013-10-01

Titre:

Transformation de programme et protection de la propriété intellectuelle - Préparation, intégration et vérification

Directeur de thèse: **Éric Filiol**
Responsable scientifique entreprise: **Patrick Hebrard**

Jury

M. Hervé Debar,	Rapporteur
M. Roberto Di Cosmo,	Rapporteur
M. Pascal Junod,	Rapporteur
M. Johann Barbier,	Examinateur
M. François Déchelle,	Examinateur
M. Jean-Marc Steyaert,	Examinateur
M. Laurent Comte,	Invité

Transformation de programme et protection de la propriété intellectuelle - Préparation, intégration et vérification

Résumé

Dans le domaine de la Défense, les contrats export s'accompagnent souvent de transferts de technologie. Un compromis est donc nécessaire entre la protection de la propriété industrielle, celle du secret national et les demandes client. Nous étudierons dans ce contexte et au sein de DCNS les transformations de sécurisation de programme, principalement l'obfuscation et le watermarking. Nous présenterons ces transformations et les principaux résultats théoriques qui les concernent, ainsi que leur adéquation au besoin de sécurité. Nous étudierons la formalisation et la mise en œuvre des principales techniques connues de transformations. Celles-ci ont pour objectif de rendre difficile la rétro-ingénierie tout en préservant les fonctionnalités et les performances des systèmes. Nous aborderons les grandes familles existantes et leur implémentation à travers le bytecode Java. Ensuite, nous étudierons l'intégration de ces techniques dans le cycle de développement d'un logiciel complexe. Un premier focus sera effectué sur la mise en œuvre de certaines techniques de transformation où leurs limites seront exhibées et des pistes d'amélioration proposées. Nous présenterons l'outillage réalisé pour cette analyse et les perspectives d'utilisation envisagées. Enfin, nous présenterons les mécanismes déployés en amont de la transformation permettant d'intégrer au plus tôt la gestion des contraintes et en aval pour vérifier que les techniques utilisées sont conformes à celles demandées afin de renforcer la confiance dans les transformations effectuées.

Mot-clefs : transformation de programme, transfert de technologie, obfuscation, watermarking

Abstract

In the military field, exportations contracts are more and more tied with transfer of technology. A compromise between intellectual property protection, national sensitive information disclosure and client requests has to be reached. We will consider in this context, and more precisely within DCNS and their combat management system, software securing transformations, and more specifically obfuscation and watermarking. We will introduce these transformations, the major theoretical results associated and how they fit with security needs. We will study formalization and implementation of main known transformation techniques. Their goal is to make reverse-engineering harder while preserving functionalities and performance characteristics. Main categories and implementation in Java bytecode will be discussed. Then, integratation of these techniques into complex software development lifecycle will be discussed. First, we will present an in-depth analysis of some techniques, showing limits and potential improvements. will be shown. Tools developed for this analysis will be introduced together with considered future use. Finally, in order to take into account the whole transformation process, we will present the actions taken before transformation in order to include as soon as possible constraints management and a downstream phase checking the correct execution of the transformation.

Keywords : program transformation, transfert of technology, obfuscation, watermarking