Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Institut National de Formation en Informatique

(INI) Oued Smar

MEMOIRE

Pour l'obtention du diplôme de

MAGISTER EN INFORMATIQUE

(Option Systèmes d'Informations)

Vérification formelle des propriétés de sécurité des logiciels

Réalisé par : M^elle^ MOHAND OUSSAID Linda

Devant le jury composé de :

Président	: Mme H. DRIAS	Professeur à l'USTHB
Rapporteur	: Mr M. AHMED NACER	Professeur à l'USTHB
Examinateur	: Mme A. AISSANI	Professeur à l'USTHB
Examinateur	: Mr M. KOUDIL	Maître de conférence à l'INI

INI, 2006

Résumé

Cette thèse présente une démarche de vérification formelle des propriétés de sécurité des logiciels. En effet, après étude des approches possibles : preuve formelle et model checking, nous avons identifié le model checking comme étant l'approche la plus adéquate pour notre problématique. Ainsi, la démarche proposée est fondée sur une combinaison de la technique de model checking et des mécanismes : d'annotation et d'abstraction basés sur l'interprétation abstraite.

Pour procéder au model checking, nous avons commencé par exprimer les propriétés de sécurité (confidentialité, intégrité, disponibilité) dans une logique temporelle appropriée. Ensuite, nous avons spécifié les systèmes auxquels pouvait s'appliquer notre démarche à savoir : les systèmes dont l'évolution peut être assimilée à un programme impératif réduit aux structures de contrôle de base.

Moyennant deux étapes : la première qui enrichit le code source par des informations relatives à la propriété à vérifier et la deuxième qui débarrasse le code source enrichi des informations superflues à la vérification de la propriété de sécurité, nous avons transformé le code source d'un programme impératif en un programme abstrait qui exhibe les instructions concernées par les propriétés à vérifier tout en faisant abstraction du reste.

L'annotation aussi bien que l'abstraction ont été développées par interprétation abstraite autour d'une correspondance de Galois qui assure que le programme abstrait correspond au programme initial.

Cette démarche a été illustrée par un exemple qui consiste en un gestionnaire de transactions bancaires simplifié.

Mots clés

Vérification formelle, model checking, propriétés de sécurité, interprétation abstraite.

Abstract

This thesis presents a formal verification of software security properties. After a brief study of the possible approaches : formal proof and model checking, we identified the model checking as being the most adequate approach for our problem. Indeed, the proposed approach is founded on a combination of the model checking technique and mechanisms : of annotation and abstraction based on abstract interpretation.

To proceed to the model checking, we started by expressing the security properties (confidentiality, integrity, availability) in an appropriate temporal logic. Then, we specified the systems to which our approach could be applied : systems whose evolution can be comparable with an imperative program reduced to the basic control structures.

By means of two stages : the first which enriches the source code by information relating to the property to be checked and the second which disencumber the enriched source code of superfluous information to the checking of the security property, we transformed the source code of an imperative program into an abstract program which exhibits instructions concerned with the properties to check while disregarding remainder.

The annotation as well as the abstraction, were developed by abstract interpretation around a Galois connection which ensures that the abstract program corresponds to the initial program.

This approach is illustrated by an example which consists of a simplified banking transactions manager.

Keywords

Formal verification, model checking, security properties, abstract interpretation

TABLE DES MATIERES