FONDEMENT DES SYSTÈMES INFORMATIQUES

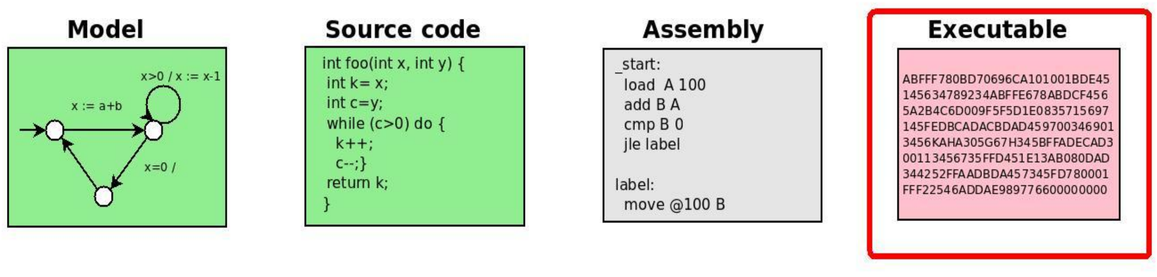
BINCOA: BINary Code Analysis

ANR ARPEGE 2008

AGENCE NATIONALE DE LA RECHERCHE
ANR

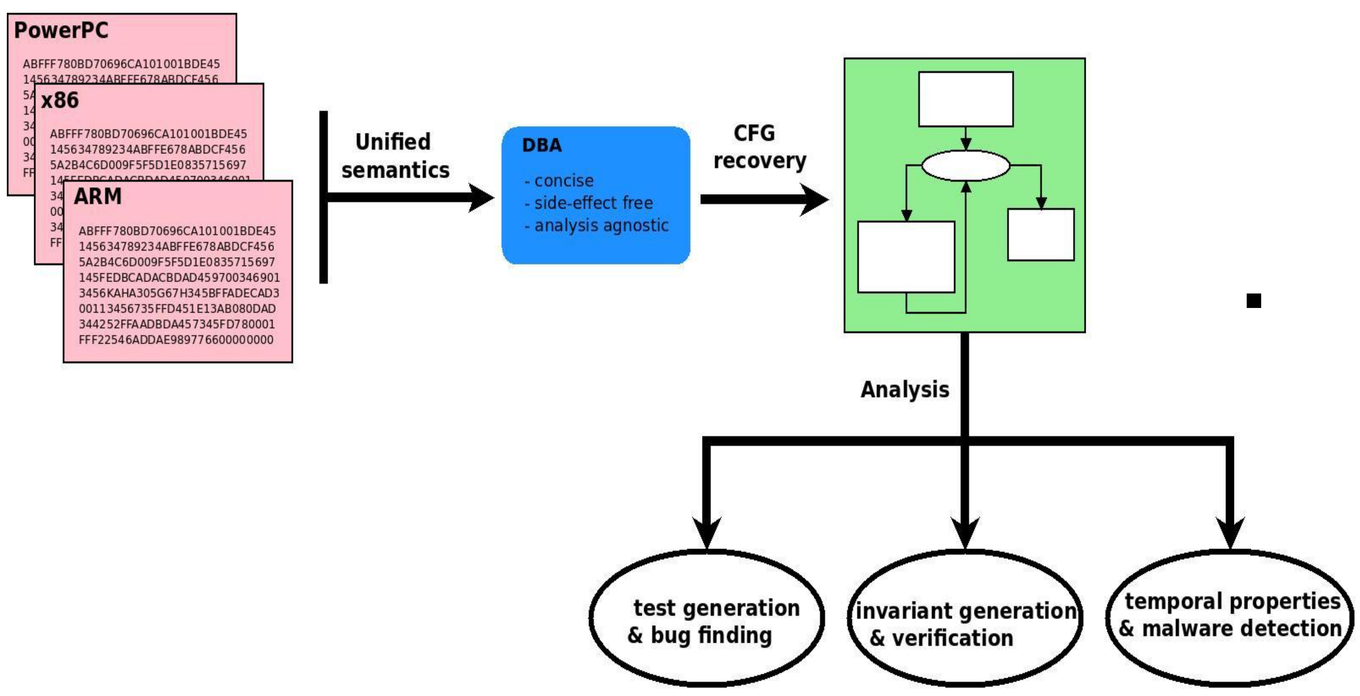
OBJECTIFS DU PROJET

L'analyse de programmes **au niveau du code binaire** et non du langage source est une problématique émergente, dont les applications industrielles concernent la **sûreté** (composant sur étagère, prise en compte de la compilation) et la **sécurité** (code mobile, malware).



BINCOA est un projet de recherche fondamentale visant à développer des méthodes d'analyse de programmes disponibles sous forme binaire :

- définir un modèle formel adapté à l'analyse de code exécutable ;
- concevoir des méthodes d'analyse pour des propriétés standard de vérification.



MÉTHODOLOGIE ET RESULTATS

Les techniques développées se basent sur des approches dynamiques et statiques (model checking, interprétation abstraite, exécution symbolique). Les partenaires industriels du projet amènent la connaissance métier et orientent les travaux vers des thèmes porteurs.

Principaux résultats :

- modèle formel concis bien adapté à l'analyse formelle de code exécutable
- reconstruction sûre du graphe de flot de contrôle d'un exécutable
- génération de tests à partir de binaires
- méthode robuste de détection de malware
- 6 prototypes testés sur des études de cas
- 13 publications internationales

CONCLUSION ET PERSPECTIVES

- BINCOA a permis des avancées notables en analyse formelle de code exécutable. Ces résultats ont été implantés et testés sur des exemples réalistes, fournis par les partenaires industriels du projet.
- Ce projet a permis de développer en France une communauté de compétences en analyse formelle de code binaire, à un moment où cette thématique émerge au niveau international.

BINCOA 0010 1010
Binary code analysis

COORDINATEUR : CEA LIST
PARTENAIRES : CEA LIST, Uni. Paris 7, Uni. Bordeaux 1, EDF, SAGEM, Trusted Labs

CONTACT :
Sébastien Bardin
sebastien.bardin@cea.fr

DE LA RECHERCHE À L'INDUSTRIE cea
UNIVERSITÉ BORDEAUX 1 Sciences Technologies
université PARIS DIDEROT PARIS 7
eDF
Trusted Labs
SAFRAN Sagem

LES RENCONTRES DU NUMÉRIQUE
17 et 18 avril 2013