OBFUSCATION PAR EXPRESSIONS MIXTES ARITHMÉTICO-BOOLÉENNES: RECONSTRUCTION, ANALYSE ET OUTILS DE SIMPLIFICATION PAR MADAME NINON EYROLLES

Discipline : Informatique Laboratoire : Laboratoire de Mathématiques de Versailles (LMV) - UMR 8100

Résumé :
L'obfuscation de logiciels est une technique de protection de programmes qui transforme du code pour rendre son analyse plus difficile. Les expressions mixtes arithmético-booléennes (MBA) sont présentées comme une bonne obfuscation du flot de données. Le domaine de l'obfuscation MBA étant assez jeune, il bénéficie de peu de littérature sur la conception et l'analyse de telles expressions obfusquées. Ainsi, beaucoup de sujets intéressants apparaissent lors de son étude, autant sur l'obfuscation que sur la désobfuscation (ou simplification) d'expressions MBA. Durant nos recherches, nous avons structuré le sujet de l'obfuscation MBA, le reliant à d'autres domaines comme la cryptographie ou la réécriture. Nous avons également reconstruit une technique d'obfuscation MBA à partir d'échantillons publics. Nous avons étudié ce que signifie simplifier

une expression obfusquée, et défini nos propres métriques de simplicité pour les expressions MBA. L'étude de la simplification MBA a entraîné l'implémentation de deux outils de désobfuscation, qui ont simplifié avec succès plusieurs examples publics d'expressions obfusquées. Finalement, nous avons évalué la résilience de l'obfuscation MBA par rapport à nos algorithmes de simplification (ainsi que d'autres techniques de désobfuscation), et nous avons conclu que la technique d'obfuscation MBA offrait peu de résilience en l'état. Nous avons donc proposé quelques pistes pour améliorer ce type d'obfuscation.

INFORMATIONS COMPLÉMENTAIRES

Membres du jury :
M. Louis GOUBIN, Professeur, université de Versailles-Saint-Quentin-en-Yvelines, FRANCE - Directeur de these
Mme Caroline FONTAINE, Chargée de recherche, CNRS, FRANCE - Rapporteur
M. Pascal JUNOD, Professeur, University of Applied Sciences Western Switzerland (HES-SO), SUISSE - Rapporteur
Mme Marion VIDEAU, responsable scientifique (maîtresse de conférences détachée), Quarkslab / LORIA, FRANCE - Examinateur
M. Renaud SIRDEY, Directeur de recherche, Commissariat à l'énergie atomique et aux énergies alternatives (CEA), FRANCE - Examinateur
M. Emmanuel FLEURY, Maître de conférences, Université de Bordeaux , FRANCE - Examinateur
Mme Sandrine BLAZY, Professeur, Université de Rennes 1, FRANCE - Examinateur
M. Johannes KINDER, Senior Lecturer, Royal Holloway, University of London, ROYAUME-UNI - Examinateur

Contact : DSR - Service FED : theses@uvsq.fr