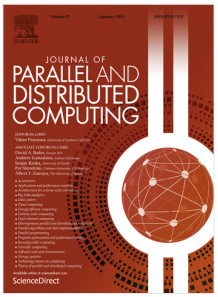
Accepted Manuscript



Evaluating model checking for cyber threats code obfuscation identification

Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, Arun Kumar Sangaiah, Aniello Cimitile

PII: S0743-7315(18)30263-6
DOI: https://doi.org/10.1016/j.jpdc.2018.04.008
Reference: YJPDC 3871

To appear in: *J. Parallel Distrib. Comput.*

Received date : 25 November 2017
Revised date : 2 March 2018
Accepted date : 13 April 2018

Please cite this article as: F. Martinelli, F. Mercaldo, V. Nardone, A. Santone, A.K. Sangaiah, A. Cimitile, Evaluating model checking for cyber threats code obfuscation identification, *J. Parallel Distrib. Comput.* (2018), https://doi.org/10.1016/j.jpdc.2018.04.008

Evaluating Model Checking for Cyber Threats Code Obfuscation Identification

Fabio Martinelli[a], Francesco Mercaldo[a], Vittoria Nardone[b], Antonella Santone[c], Arun Kumar Sangaiah[d], Aniello Cimitile[b]

[a] *Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy*
[b] *Department of Engineering, University of Sannio, Benevento, Italy*
[c] *Department of Bioscience and Territory, University of Molise, Pesche (IS), Italy*
[d] *School of Computing Science and Engineering, VIT University, Vellore 632014, India*

Abstract

Code obfuscation is a set of transformations that make code programs harder to understand. The goal of code obfuscation is to make reverse engineering of programs infeasible, while maintaining the logic on the program. Originally, it has been used to protect intellectual property. However, recently code obfuscation has been also used by malware writers in order to make cyber threats easily able to evade antimalware scanners. As a matter of fact, metamorphic and polymorphic viruses exhibit the ability to obfuscate their code as they propagate. In this paper we propose a model checking-based approach which is able to identify the most widespread obfuscating techniques, without making any assumptions about the nature of the obfuscations used. We evaluate the proposed method on a real-world dataset obtaining an accuracy equal to 0.9 in the identification of obfuscation techniques.

Keywords: obfuscation, Android, model checking, formal methods, malware

Email addresses: fabio.martinelli@iit.cnr.it (Fabio Martinelli), francesco.mercaldo@iit.cnr.it (Francesco Mercaldo), vnardone@unisannio.it (Vittoria Nardone), antonella.santone@unimol.it (Antonella Santone), arunkumarsangaiah@gmail.com (Arun Kumar Sangaiah), cimitile@unisannio.it (Aniello Cimitile)