World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:09, 2018

A Software Engineering Methodology for Developing Secure Obfuscated Software

Authors : Carlos Gonzalez, Ernesto Linan

Abstract : We propose a methodology to conciliate two apparently contradictory processes in the development of secure obfuscated software and good software engineered software. Our methodology consists first in the system designers defining the type of security level required for the software. There are four types of attackers: casual attackers, hackers, institution attack, and government attack. Depending on the level of threat, the methodology we propose uses five or six teams to accomplish this task. One Software Engineer Team and one or two software Obfuscation Teams, and Compiler Team, these four teams will develop and compile the secure obfuscated software, a Code Breakers Team will test the results of the previous teams to see if the software is not broken at the required security level, and an Intrusion Analysis Team will analyze the results of the Code Breakers Team and propose solutions to the development teams to prevent the detected intrusions. We also present an analytical model to prove that our methodology is no only easier to use, but generates an economical way of producing secure obfuscated software.

Keywords : development methodology, obfuscated software, secure software development, software engineering
Conference Title : ICACET 2018 : International Conference on Advances in Computer Engineering and Technology
Conference Location : Prague, Czechia
Conference Dates : September 03-04, 2018