The Dark Side of Software Reverse Engineering

Donald J. Reifer, President
Reifer Consultants, Inc., USA
don@reifer.com

Abstract

During the past decade, substantial advances have been made in the field of software reverse engineering. Tools and techniques that have been developed for program understanding, design recovery and reengineering and/or refactoring have been commercialized and deployed to reduce the software maintenance burden. However, along with the good comes the dark side of software reverse engineering. These same tools and techniques can be and have been used for nefarious purposes. Take the disassemblers/debuggers used for exploring binary programs for which source code is not available. Besides being able to figure out what functions the software performs and in what manner, these tools can be used to identify sensitive information hidden in the code (data, algorithms, etc.). For example, such tools can be used to get at this sensitive information even when it is guarded, obfuscated or encrypted. In addition, those tools and techniques employed to figure out how a program works can also be used to determine how it breaks. For example, exploiters can use the same exceptions that were put into the code to improve safety to crash the system. The challenge posed to the reverse engineering community is to find ways to prevent the misuse of their technology along with its proper use.