СПИСОК ЛИТЕРАТУРЫ:

1. *Wolfengagen V. E.* Applicative computing. Its quarks, atoms and molecules / Edited by Dr. L. Yu. Ismailova. Moscow: «Center JurInfoR», 2010. — 62 p.
2. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В.* Структура компьютинга и конструирование вычисления // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2010. № 08. URL: http://technomag.edu.ru/doc/153062.html (дата обращения: 15.12.2012).
3. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В.* Модель вычислений, чувствительная к семантической нестабильности // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2010. № 12. URL: http://technomag.edu.ru/doc/163548.html (дата обращения: 15.12.2012).
4. *Исмаилова Л. Ю., Косиков С. В., Вольфенгаген В. Э., Зинченко К. Е.* Средства инструментальной поддержки композиции и специализации предметно-ориентированных механизмов наследования для правовых деловых игр // В мире научных открытий. 2010. № 1—4. С. 32—36. URL: http://nkras.ru/vmno/issues/articles/2010/1-4.pdf (дата обращения: 15.12.2012).
5. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В., Лаптев А. Д., Назаров В. Н., Рословцев В. В., Сафаров И. С., Степанов А. Л.* Аппликативный компьютинг: попытки установить природу вычислений // Вестник Удмуртского университета. Сер. 1: Математика. Механика. Компьютерные науки. Электрон. журн. 2009. Вып. 2. С. 110—117. URL: http://vst.ics.org.ru/uploads/vestnik/2_2009/vu09213.pdf (дата обращения: 15.12.2012).
6. *Вольфенгаген В. Э., Исмаилова Л. Ю., Косиков С. В., Лаптев А. Д., Назаров В. Н., Рословцев В. В., Сафаров И. С., Степанов А. Л.* Комбинаторы: объекты, помогающие понять строение компьютинга // Вестник Удмуртского университета. Сер. 1: Математика. Механика. Компьютерные науки. Электрон. журн. 2009. Вып. 2. С. 118—131. URL: http://vst.ics.org.ru/uploads/vestnik/2_2009/vu09214.pdf (дата обращения: 15.12.2012).

Е. И. Гончаров

АВТОМАТИЧЕСКАЯ ДЕОБФУСКАЦИЯ ИСПОЛНЯЕМОГО КОДА, ЗАЩИЩЕННОГО С ПРИМЕНЕНИЕМ ВИРТУАЛЬНЫХ МАШИН

Обфускация, или запутывание кода, — это модификация кода программы таким образом, что она полностью сохраняет свою функциональность, но анализ и понимание алгоритмов ее работы значительно усложняются. Обфускация может применяться как для защиты законных интересов (например, для сокрытия авторских алгоритмов), так и для маскировки недекларированных возможностей ПО. Причем использование запутывания кода во вредоносном ПО в настоящий момент крайне широко распространено. Таким образом, для анализа подобных программ автоматизирование деобфускации, или «распутывания кода», является актуальной проблемой.

Для деобфускации бинарного кода, запутанного с использованием непрозрачных предикатов, свойства полиморфизма и добавления «мертвого» кода, достаточно успешно применяются методы символьного исполнения и абстрактной интерпретации [1]. В то же время код, защищенный с помощью виртуальных машин, все еще представляет серьезную проблему, так как успешность анализа сильно зависит от опыта аналитика. В этой работе описывается разрабатываемый автоматический метод деобфускации виртуальных машин класса «decode-dispatch», в основе которого лежат указанные методы символьного исполнения и абстрактной интерпретации, учитывающие характерные особенности данного класса. В случае успеха в разработке данного метода решение этой актуальной задачи перейдет из разряда трудоемких в разряд примитивных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Udupa S. K., Debray S. K., Madou M.* Deobfuscation: Reverse Engineering Obfuscated Code // 12th Working Conference on Reverse Engineering, 2005. С. 45-54.