

МЕТОДЫ АНАЛИЗА ОБФУСЦИРОВАННЫХ ПРОГРАММ

М.А. Бартошик

Изучение методов анализа обфусцированных программ является необходимым шагом в разработке надежных методов защиты программного обеспечения. Данные методы делятся на несколько групп [1]: динамические, статические, статистические, синтаксические. Динамические методы основаны на наблюдении за поведением программы на конкретных наборах входных данных (например, отладка программы с использованием инструментальных средств). Методы статического анализа основаны на изучении графа потока управления программы и графа потока данных. Данные методы работают с исходным кодом программы (например, поиск запутывающих конструкций на основе известных шаблонов). Методы статистического анализа собирают информацию о выполнении запутанной программы на различных наборах входных данных (например, анализ покрытия исходного кода, анализ трасс выполнения). Используя результаты статистических методов анализа можно, например, определить участки с недостижимым кодом. Синтаксические методы основаны на лексическом, синтаксическом и семантическом анализе программ.

Данные группы методов успешно применяются для выявления и устранения запутывающих преобразований. Например, для устранения развернутых циклов строится граф потока управления и анализируется на предмет наличия повторяющихся конструкций. При обнаружении циклов производится их свертка. Синтаксический анализ позволяет выделить известные непрозрачные предикаты по образцу. Статистический анализ позволяет изучать покрытие кода при различных входных данных и выделять участки с потенциальным «мертвым» кодом. При поиске объединенных функций проводится статистический анализ трасс выполнения. При наличии четкого разделения на две альтернативные трассы производится разделение функций.

Таким образом, наличие большого числа методов анализа обфусцированных программ указывает на необходимость совершенствования методов обфускации и разработки надежных методов оценки эффективности запутывающих преобразований.

Литература

1. Чернов А.В. Анализ запутывающих преобразований программ. // Труды Института системного программирования РАН. – 2003.

КОМБИНИРОВАННОЕ МАРКИРОВАНИЕ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ТРИАНГУЛЯЦИОННЫХ КЛЮЧЕВЫХ ТОЧЕК

А.А. Борискевич, П.М. Никуленко, Аль-Асади Мохайман Салах Абдулмахди

В настоящее время не существуют эффективных методов для защиты авторских прав владельца мультимедийного 2D/3D контента (текстовые сообщения, изображения, видео, гибридные изображение/текст и т.д.), обеспечивающих компромисс между устойчивостью к широкому классу преднамеренных и непреднамеренных воздействий, перцептуальной и статистической невидимостью и емкостью внедрения. Кроме того, известные методы маркирования являются значительно сложнее для текстовых документов, чем для изображений и могут быть использованы только для цифровых медиаданных без возможности их представления на твердом носителе.

Предложен алгоритм, основанный на формировании множества особых точек с учетом механизмов восприятия зрительной информации, непересекающихся множеств точек вокруг каждой из особых точек и триангуляционных окрестностей маркирования, правилах выбора позиций и параметров ключевых точек и внедрения данных с учетом динамического диапазона маркируемого контента, параметров ключевых точек и идентификационных параметров синусоидальных решеток, используемых для кодирования встраиваемых данных.

Осуществлена программная реализация предложенного алгоритма на языке C++. Результаты моделирования маркирования текстовых документов, космических и медицинских изображений, гибридных изображение/текст показывают, что алгоритм позволяет управлять