## 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 основы 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 покрытие 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 участи 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

количеством особых точек и идентификационных параметров синусоидальных решеток для повышения емкости внедрения, обеспечивает устойчивость к атакам типа «печать-сканирование», масштабирование (0,5…1,5 раза), поворот (300, 750, 1800), смещение (сдвиг на любое число пикселов).

## АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ОНЛАЙН-МАГАЗИНЕ ZORBASHOP.COM

В.А.Вишняков, Храйба Мохаммед

В докладе представлены используемые методы защиты информации в онлайн-магазине (zorbashop.com). Выделены следующие направления защиты: метод шифрования с цифровой подписью, использование брандмауэра, защищенный протокол Secure Sockets Layer (SSL), разрешение доступа.

Метод шифрования: использован алгоритм MD5 и кэш для хранения паролей, MD5 - это алгоритм, который, использует в качестве входных данных сообщение произвольной длины и выдает на выходе 128-битовое значение. Вводимые данные последовательно разбиваются на блоки по 512 бит. В алгоритме MD5 используются массив значений T[*i*], $i = 1, 2, \ldots, 64$. Кэш содержит случайные данные, которые используются как дополнительный вход в систему. Хэш-функция, которая хэширует пароль. Основная функция кэша — защита от символьных атак против списка хэш-паролей и против заранее вычисленных в таблице атак.

Брандмауэр создает дополнительный слой безопасности по всему Интернет-магазину. С помощью правила брандмауэра, он будет блокировать нападавших или вносить их в черные списки и запрещать им доступ к сайту. Он имеет сканер для предоставления рекомендации о установке в нашем магазине.

Защищенный протокол: Secure Sockets Layer (SSL) используя протокол защищенных Сокетов (SSL) с ключом шифрования длиной 128-бит (самый высокий уровень, имеющихся в продаже).

Капча (CAPTCHA) — это визуальное средство, которое гарантирует, что человеческое существо, а не компьютер взаимодействует с сайтом. Капча может быть использован как для администратора так и для клиентов.

## ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ МЕЖСЕТЕВОГО ЭКРАНА CISCO ASA 5520

Р.М. Горбуль

Корпоративная сеть является неотъемлемой частью любой современной компании. Корпоративная сеть требует высокого уровня защиты, которую может обеспечить межсетевой экран Cisco ASA 5520. Данный межсетевой экран является аппаратным средством обеспечения защиты. Произведен анализ функций и возможностей межсетевого экрана. Межсетевой экран обеспечивает пропускную способность 450 Мбит/с для не зашифрованного трафика и 225 Мбит/с для зашифрованного. Опытным путем было выявлено, что межсетевой экран выдерживает документированную пропускную способность как для не зашифрованного, так и зашифрованного видов трафика, что является отличным показателем для такого класса устройств. При помощи средств виртуализации были смоделированы режимы работы Active/Active и Active/Standby двух межсетевых экранов в связке для тестирования отказоустойчивости. Была смоделирована конфигурация с использованием нескольких контекстов или другими словами, несколькими виртуальными брандмауэрами, каждый со своей конфигурацией и логическими интерфейсами. Также была исследована функция глубокого анализа протоколов прикладного уровня и проверена поддержка протоколов динамической маршрутизации OSPF и EIGRP. Межсетевой экран Cisco ASA 5520 обеспечивает высокий уровень защиты для корпоративных сетей среднего и малого бизнеса.