ОТЗЫВ

официального оппонента на диссертацию Лубкина Ивана Александровича «Метод снижения подверженности приложений к реализации уязвимостей за счет обфускации машинного кода», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Актуальность работы

Несмотря на то, что процесс разработки ПО регламентируется множеством стандартов и требований, направленных на обеспечение качества, разработчики и архитекторы продолжают допускать ошибки при разработке программных продуктов. Такие ошибки, в свою очередь, могут порождать серьезные дефекты, связанные с безопасностью информационных систем, в которых будут функционировать такие программные средства. Особенным типом уязвимостей являются те, которые позволяют осуществить удаленное исполнение кода, так как при их использовании атакующий может выполнять произвольные алгоритмы. Актуальность защиты от таких уязвимостей обусловлена распространенностью подверженных им архитектур (в частности, AMD64) и отсутствием решений, обеспечивающих устранение принципиальной возможности реализации атак. Применимость существующих средств защиты снижает то, что для их использования в подавляющем большинстве требуется наличие исходных текстов программ, что приводит к необходимости ожидания внесения исправлений от разработчика.

Таким образом, тема диссертационной работы является актуальной и обусловлена рядом вышеописанных факторов, которые порождают серьезные или критические риски информационной безопасности для информационной системы, в которой функционирует уязвимый программный продукт.

Краткий обзор и анализ содержания работы

Во введении обосновывается актуальность темы диссертации, формулируются цель и задачи исследования, обсуждаются научная новизна и практическая ценность выносимых на защиту результатов, даётся краткая характеристика содержания работы.

В первой главе соискателем рассмотрены проблематика *RoP*-уязвимостей и недостатки существующих подходов по защите от них. В рамках этого приведены результаты анализа выборки уязвимостей соответствующего типа и сформулирована модель атак. Далее выделены существующие методы защиты, а также их недостатки; сформулированы требования для модификации существующих подходов, что позволит повысить

защищенность программ от уязвимостей. Наконец, приведена информация об организации программ, которая должна учитываться при решении сформулированного ранее требования по встраиванию системы защиты даже при отсутствии исходных текстов защищаемого приложения.

Во второй главе представлена модель работы программ, описывающая процесс выполнения как композицию функций, обеспечивающую преобразование данных. Далее проанализировано, какие данные являются наблюдаемыми для окружения программы, что положено в основу неразличимости поведения (формируемых данных) двух приложений: оригинального и с зарезервированными для системы защиты участками. На основании критерия неразличимости предложены условия модификации, при выполнении которых результаты работы модифицированной программы не будут отличаться от оригинального приложения. Наконец, предложен алгоритм резервирования в программе участков, куда будет в дальнейшем встроен код системы защиты, который не приводит к искажению логики работы приложения.

В третьей главе предложены метод снижения подверженности приложений к реализации уязвимостей и алгоритм преобразования для обеспечения этого. В рамках него производится как устранение пригодных для проведения атак участков, так и защита графа потока управления для участков, из которых не могут быть удалены опасные инструкции. Приведены алгоритм устранения опасных значений и методика контроля целостности адреса возврата из подпрограмм.

В четвертой главе рассмотрены существующие методы оценки защищенности и сделан вывод о том, что для предлагаемого метода защиты наиболее близок метод подсчета гаджетов, рассмотрены его недостатки. На основании этих результатов и с учетом сформулированной в первой главе модели атаки предложен модифицированный метод оценки защищенности. В рамках него вводится показатель возможностей атакующего (метрика защищенности), показывающий состав доступных системных вызовов и подпрограмм.

В пятой главе приводятся детали программной реализации предложенного метода снижения подверженности приложений к *RoP*-уязвимостям, а также результаты сравнения с существующими средствами защиты. В частности, приведены результаты качественного сравнения с аналогами, которое показало большую защищенность предложенной защиты, а также сравнения предложенного решения с публично доступными аналогами, показавшее большую защищенность и сравнимое падение производительности для приложений, защищенных в соответствии с предлагаемым методом. В конце главы приведены результаты внедрения результатов работы.

В заключении сформулированы основные результаты, полученные соискателем, а также представлены перспективы дальнейшей разработки темы.

Общий объем работы составляет 179 страниц, содержащих введение, 5 глав, заключение, список литературы из 104 наименований, приложения, а также список используемых терминов и сокращений.

Научная новизна полученных результатов

В диссертационной работе были разработаны:

1. Модифицированный метод снижения числа пригодных для проведения *RoP*-атак участков в программах, отличающийся от существующих предложенной новой моделью вычислений и впервые сформированными на её основе критериями и условиями неразличимости алгоритмов программ.
2. Модифицированная методика контроля целостности графа потока управления, отличающаяся от аналогов устойчивостью к фрагментарному раскрытию содержимого стека значений за счет использования псевдослучайных значений с их защитным связыванием для соседних фреймов программ.
3. Модифицированный метод оценки эффективности систем защиты программ от *RoP*-атак, отличающийся от аналогов введением метрики защищенности, показывающей потенциал проведения атаки за счет графа передачи данных до целевых с точки зрения атакующего регистров. Предложенный подход основан на модели атак, обобщающей выборку публично доступных эксплойтов.

Теоретическая и практическая значимость

Разработанный в ходе работы метод снижения подверженности приложений к реализации уязвимостей удаленного исполнения кода и программная реализация средства защиты могут быть использованы как при разработке, так и при эксплуатации программного обеспечения. Предложенный способ генерации псевдослучайных значений обеспечивает контроль графа потока управления, устойчивого к примитивам чтения.

Полученные в рамках экспериментального анализа эффективности результаты показали, что разработанное решение позволяет снизить как разнообразие, так и количество гаджетов в защищаемом приложении. При этом оставшиеся после применения защиты гаджеты непригодны для проведения атак, что было показано на заведомо уязвимом приложении. Внесенные в него уязвимости переполнения буфера (как в стеке, так и в куче) и примитив чтения позволяют до применения предлагаемого метода защиты успешно выполнять *RoP*-атаку с обходом таких механизмов защиты, как *ASLR* и *StackGuard*. После защиты перестает приводить к перехвату

управления переполнение буфера в стеке, а переполнение буфера в куче хоть и приводит к перехвату управления, но не приводит к успешной атаке из-за отсутствия необходимых гаджетов.

Разработанное программное средство было внедрено в технологический процесс разработки программного обеспечения в СФУ и в учебный процесс СибГУ им. М.Ф. Решетнева. Кроме того, защищенное с использованием предлагаемого метода приложение с закрытым исходным кодом прошло успешную тестовую эксплуатацию в коммерческой организации, что подтвердило отсутствие искажений в логике его работы.

Обоснованность и достоверность полученных результатов и выводов

Достоверность работы подтверждается результатами, полученными с использованием предлагаемого в работе решения и их сопоставлением с имеющимися современными теоретическими и экспериментальными данными, полученными другими авторами в этой области. Для контроля качества анализа защищаемого программного обеспечения используется являющийся стандартом де-факто дизассемблер IDA, а разработанный и реализованный план тестирования обеспечивает качество реализации предложенной методики.

Рекомендации по использованию результатов

Полученные в работе результаты могут использоваться для интеграции в цикл безопасной разработки программного обеспечения. Так как предложенное автором решение эффективнее аналогов, интегрируемых на этапе компиляции, то оно может использоваться для повышения защищенности приложений от эксплуатации уязвимостей.

Соответствие содержания диссертации содержанию автореферата

Содержание автореферата диссертации соответствует содержанию диссертации и полностью отражает полученные в ней практические и теоретические результаты и выводы.

Полнота опубликования результатов работы, соответствие автореферата содержанию диссертации

Основные положения и результаты работы были опубликованы в 14 научных статьях и тезисах докладов. Из них 7 публикаций в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных ВАК, 3 статьи индексируются в международной базе Scopus.

По теме работы было получено 2 свидетельства на регистрацию программы для ЭВМ и БД. Работа по теме диссертации проводилась в

рамках одного гранта и в рамках базовой части одного государственного задания.

Выборочный анализ выполненных автором работ позволяет заключить, что все основные результаты работы в полной мере отражены в публикациях автора.

Соответствие темы диссертации заявленной научной специальности

Содержание представленной работы соответствует паспорту специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность» по следующим пунктам:

п.15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

п.5. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.

п.11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

По диссертации имеются следующие замечания

1. В пункте 5.5.1 приведено описание совместного применения для одного и того же приложения как программной реализацией предлагаемого автором средства защиты, так и существующим средством защиты *StackGuard*. Не приведено пояснение возможного корректного совместного использования, так как *StackGuard* использует сегментный регистр *FS* для нахождения блока управления процессом, но в ограничениях на структуру рассматриваемых программ (подраздел 2.1) указано использование плоской модели сегментации.
2. На странице 35 в первом дефисе указано, что из рассмотрения исключаются приложения, содержащие написанные вручную ассемблерные вставки. При этом в незначительном наборе системных библиотек операционных систем имеются сформированные вручную ассемблерные вставки для оптимизированного выполнения операций в рамках используемой архитектуры. В диссертации не приведен порядок защиты таких библиотек.
3. В работе имеются синтаксические и орфографические ошибки.

Заключение по работе

Отмеченные выше недостатки не влияют на общую положительную оценку работы. Диссертация является завершенной научно-квалифицированной работой на актуальную тему, обладающей научной новизной, в которой решена важная научно-техническая задача снижения подверженности приложений к реализации уязвимостей возвратно-ориентированного программирования. По своему содержанию работа отвечает критериям, которым должна отвечать диссертационная работа, изложенным в «Положении о порядке присуждения ученых степеней» ВАК России, утвержденном постановлением Правительства РФ № 842 от 24.09.2013, а её автор – Лубкин Иван Александрович – заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Зав. кафедрой безопасности информационных
Технологий им. О.Б. Макаревича
Института компьютерных технологий и информационной безопасности
Инженерно-технологической академии
Федерального государственного автономного
образовательного учреждения высшего образования
«Южный федеральный университет»,
к.т.н., доцент

Абрамов Евгений Сергеевич
г. Таганрог
ул. Чехова, 2, ауд. И-415
8(8634) 37-19-05
abramoves@sfedu.ru