ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ
«РОСТЕХ»
АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКАЯ ЭЛЕКТРОНИКА»

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ПРОГРАММНЫХ СРЕДСТВ»
(АО «НИИ ПС»)

ул. Политехническая, д. 22, лит. «Н»,
Санкт-Петербург, 194021
Тел. /факс (812) 313-78-00, тел. (812) 313-78-01
E-mail: office@nii-ps.ru,
E-mail: niipc@mail.ru
ОГРН 1117847048440,
ИНН / КПП 7804454896 /780201001

23.08.2017 № 91-12/2

На № _____ от _____

УТВЕРЖДАЮ
Генеральный директор
Акционерного общества
«Научно-исследовательский
институт программных
средств» (АО «НИИ ПС»),
д-р техн. наук, профессор.

_____ О.Ю. Гаценко

Отзыв ведущей организации

на диссертацию Израилова Константина Евгеньевича на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Актуальность темы выполненного диссертационного исследования

Важной особенностью большинства современных процессов является информационное взаимодействие через глобальные телекоммуникационные сети; передаваемая же информация требует определенного уровня обеспечения ее безопасности. Одним из потенциально опасных мест при этом является телекоммуникационное оборудование, обрабатывающее сетевой трафик с помощью алгоритмов. Машинный код последних может содержать в себе уязвимости (случайные и злонамеренные), ведущие к реализации угроз информации. Ситуация осложняется тем, что используемое оборудование (особенно в России) может поставляться зарубежными производителями, преследующими собственные интересы и не предоставляющими исходный код программного обеспечения. В этих условиях поиск в

машинном коде уязвимостей является крайне востребованным, поскольку большинство имеющихся решений предназначены для анализа исключительно исходного кода.

Существующие автоматически средства осуществляют поиск уязвимостей в машинном коде, которые могут быть хорошо описаны формальными правилам. Как следствие они не выявляют более «умные» программные закладки, определение которых возможно, как правило, только экспертом. Отображение алгоритмов в виде графа потока управления между процессорными инструкциями хотя и позволяет эксперту провести его исследование, тем не менее является крайне малоэффективным из-за сложности такого представления. Применение реверс-инжиниринга в виде средств декомпиляции машинного кода также нельзя считать подходящим, поскольку такой подход изначально ставит своей целью восстановление исходного кода (с возможностью его компиляции), что не соответствует цели в виде поиска уязвимостей.

В этих условиях алгоритмизация машинного кода, заключающаяся в восстановлении его архитектуры, модулей, подпрограмм и алгоритмов, может повысить эффективность поиска уязвимостей в коде (плохо формализуемых и требующих участия эксперта), что обуславливает актуальность темы диссертационного исследования Израилова К.Е.

Характеристика основных научных результатов

Автор на защиту выносит следующие основные научные результаты, обладающие новизной и достоверностью:

1) Структурная модель машинного кода с уязвимостями;
2) Метод алгоритмизации машинного кода;
3) Архитектура программного средства алгоритмизации машинного кода;
4) Комплекс научно-методических средств оценки алгоритмизации машинного кода в интересах поиска уязвимостей.

Для первого основного научного результата несомненную научную новизну представляет предложенная и обоснованная структурная S-модель машинного кода, отличная от классической линейной связыванием вместе модульной архитектуры кода и алгоритмов его подпрограмм. Также, в модели отражаются уязвимости в алгоритмах и архитектуре кода, названные по их структурному уровню – низкоуровневые, среднеуровневые и высокоуровневые.

Новизна второго научного результата состоит в предложенном новом концептуальном подходе к восстановлению архитектуры и алгоритмов машинного кода с использованием S-модели его экземпляра. Используемое для этого представление отличается от существующих предназначенностью для отражения результатов алгоритмизации. При этом, имеется возможность постепенной «подстройки» как самого представления, так и особенностей алгоритмизации под запросы эксперта.

Третий основной научный результат заключается в разработке архитектуры программного средства алгоритмизации, принципы построения которой основаны на использовании оригинальной S-модели. Также, в интересах реализации архитектуры созданы оригинальные алгоритмы для определения входных/выходных параметров функций, упрощения и оптимизации S-модели; создан работоспособный пример поиска уязвимостей в логике работы подпрограмм.

Относительно четвертого основного научного результата следует отметить, что предложен целый новый комплекс средств разносторонней оценки алгоритмизации, состоящий из методик и критериев. Первые применимы к средству алгоритмизации машинного кода и ручному способу поиска среднеуровневых и высокоуровневых уязвимостей, а вторые – к получаемому алгоритмизированному представлению.

Достоверность результатов и научных положений диссертации определяется корректностью постановки задач на исследование, строго обоснованной совокупностью ограничений и допущений, применением апробированных общенаучных и специальных методов исследования, и подтверждается результатами тестирования прототипа программного средства алгоритмизации, автоматизирующего основные этапы метода.

Совокупность полученных основных научных результатов и их характеристика позволяет сделать вывод о достижении соискателем цели своего диссертационного исследования, а именно повышении эффективности поиска уязвимостей в машинном коде телекоммуникационных устройств путем его алгоритмизации.

Значимость результатов диссертации для развития отрасли информационной безопасности и защиты информации

Полученные Израиловым К.Е. в ходе своего исследования и изложенные в диссертации результаты имеют как теоретическую, так и практическую значи-

мость для развития отрасли информационной безопасности и защиты информации.

Их теоретическая значимость определяется вкладом в развитие направления реверс-инжиниринга машинного кода с целью восстановления информации об исходном коде в части его архитектуры и алгоритмов.

Для этого автором был проведен анализ основных парадигм программирования на предмет связи их структурных особенностей (метаданных) с генерируемыми инструкциями машинного кода. На основании полученных знаний была создана схема алгоритмизации машинного кода, которая позволила синтезировать соответствующий метод, относящийся к классу используемых для восстановления исходного кода. Для реализации средства в части поддержки модели машинного кода и его преобразования в более структурно высокоуровневую форму были разработаны соответствующие объекты и процедуры работы с ними. В интересах сравнения методов и средств, используемых для алгоритмизации машинного кода, предложены критерии, по которым возможна оценка понятности получаемых представлений для эксперта, а также критерии, определяющие, насколько корректно была произведена алгоритмизация.

Практическая значимость результатов диссертации для развития отрасли информационной безопасности и защиты информации заключается в возможности получение представления машинного кода, хорошо подходящего эксперту для анализа его на предмет наличия уязвимостей. Модель машинного кода, полученная в результате его исследования на предмет содержания структурной информации об исходном коде, позволяет ставить научно-обоснованные задачи, связанные с реверс-инжинирингом и последующим поиском уязвимостей – что и было сделано для получения метода алгоритмизации. Данный метод преобразовывает экземпляр машинного кода в представление, содержащее алгоритмы и архитектуру, а также отражающее уязвимости того же структурного уровня – среднеуровневые и высокоуровневые. Поскольку возможна и целесообразна автоматизация основного этапа метода, была разработана архитектура соответствующего программного средства. На ее базе возможно создание аналогичных программных средств, обеспечивающих получение высокоуровневых представлений кода из низкоуровневых. Важной особенностью является независимость основной части архитектуры от специфики обрабатываемого кода. Методики, входящие в созданный автором

комплекс научно-методических средств оценки, могут быть использованы для выбора подходящего метода и средства алгоритмизации среди альтернатив. Фактическое применения комплекса показало преимущество метода алгоритмизации.

Можно предположить, что результаты проведенного Израиловым К.Е. исследования будут востребованы научными и проектными организациями, занимающимися вопросами обеспечения информационной безопасности, особенно в условиях проприетарности программного обеспечения большинства телекоммуникационных устройств, имеющих при этом зарубежного производителя.

Рекомендации по использованию результатов и выводов диссертации

Помимо перспектив дальнейшего развития темы исследования, аргументированно определенного автором, как разработка интерактивной среды визуализации ассемблерного кода и его восстановленного представления, создание механизма сравнения алгоритмов работы машинного кода, автоматизация поиска уязвимостей в алгоритмах и архитектуре, создание более подходящих для анализа экспертом представлений кода, считаем целесообразным дать следующие рекомендации по использованию результатов и выводов диссертации Израилова К.Е.

Во-первых, это применение алгоритмизации для анализа машинного кода не только телекоммуникационных устройств, но и такой группы программных средств разработки, как компиляторы. Дело в том, что актуализировалась угроза встраивания в средства разработки НДВ, логика работы которых производит встраивание в скомпилированный код программных закладок. Такой враждебный код в компиляторе практически невозможно обнаружить автоматическим способом, поскольку их вредоносный эффект проявляется лишь косвенно – при анализе или использовании получаемого на выходе экземпляра кода, вариаций которого может существовать бесконечное множество. В этом случае, при отсутствии открытого исходного кода компилятора (что вполне распространенная ситуация для проприетарных продуктов), необходим глубокий анализ логики его работы, которая является достаточно сложной и требующей для своего понимания использования специализированных представлений. В интересах этого может быть применен предлагаемые метод и программное средство алгоритмизации, возможно, после необходимой доработки.

И, второе, это расширение функционально-информационной структуры средства алгоритмизации (с последующей программной реализацией) для решения задачи формальной верификации алгоритмов и архитектуры программного обеспечения, ориентированной на поиск уязвимостей при участии эксперта. От последнего может потребоваться описание правил касательно принципов построения архитектуры, ограничений на взаимодействие модулей и допустимых эффектов работы алгоритмов. Программное средство должно будет выявить несоответствие логики работы машинного кода таким правилам, предоставив эксперту право принятия решения касательно уязвимостей и возможность корректировки правил. С точки зрения описанной в диссертации структуры программного средства, последнее обладает необходимым функционалом и потребуется только добавление поддержки формальных правил и их учета на дополнительной стадии верификации.

Замечания и недостатки

На основании изучения диссертационной работы Израилова К.Е. «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» можно сделать ряд замечаний и указать на некоторые недостатки, а именно:

1. Во введении диссертации недостаточно полно сформулирована задача исследования, поскольку указывается лишь путь решения проблемного вопроса – создание метода алгоритмизации машинного кода для последующего поиска уязвимостей, хотя целесообразно также указание существующих начальных и требуемых конечных условий для выполнения задачи.

2. В диссертации не уточняется понятие архитектуры, восстанавливаемой из машинного кода, что позволяет ее трактовать различными способами. Определение архитектуры, как информации о модулях программного кода и их взаимодействии, не является достаточным.

3. В п. 2.2. среди подходов к поиску уязвимостей не рассматривается подход формальной верификации программного обеспечения, в том числе применяемый для его проверки на наличие ошибок и дефектов.

4. В п. 1.3 анализируются только четыре парадигмы программирования: модульная, процедурная, структурная и императивная, исключая другие, например, функциональную или объектно-ориентированную.

5. В Приложении Г на блок-схемах алгоритмов указано излишнее количество стрелок; для стандартных направлений – сверху вниз и слева направо – стрелки указывать не обязательно. Также, приводимые в приложении алгоритмы требуют более детального описания и примеров их программной реализации.

6. В работе изредка встречается недостаточно удобочитаемое форматирование текста, например, у подпунктов «Архитектурные элементы», «Настройка алгоритмизации» и «Обобщенный пример использования» для п. 3.1 отсутствует очевидная нумерация – 3.1.1, 3.1.2 и 3.1.3, подпункт 1.3.4 и первый заголовок в подпункте 4.2.2 не имеют отступа от предыдущего текста и др.

Заключение

Несмотря на вышеуказанные замечания и недостатки, диссертация выполнена на высоком научном уровне и содержит новые, достоверные и значимые результаты. Результаты выполненного Израиловым К.Е. исследования несомненно имеют значение для современного развития телекоммуникационных сетей и обеспечения их информационной безопасности, а также могут быть непосредственно использованы для защиты информации при ее обработке машинным кодом. Личный вклад автора в получении результатов несомненен.

Все положения, выносимые на защиту, прошли широкую апробацию и опубликованы в достаточной степени в рецензируемых изданиях.

С учетом вышеизложенного можно сделать вывод, что диссертация Израилова Константина Евгеньевича на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» является законченной научно-квалификационной работой, в которой содержится решение научной задачи по разработке метода и средства алгоритмизации машинного кода в интересах поиска среднеуровневых и высокоуровневых уязвимостей в программном обеспечении телекоммуникационных устройств, имеющей значение для развития отрасли информационной безопасности и защиты информации.

Таким образом, диссертация соответствует п. 9 «Положения о порядке присуждения ученых степеней», а ее автор заслуживает присуждения ученой степени

кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Диссертация Израилова К.Е. на тему «Метод алгоритмизации машинного кода для поиска уязвимостей в телекоммуникационных устройствах» и отзыв на нее обсуждены и одобрены на заседании научно-технического совета АО «НИИ ПС» 23 августа 2017 года, протокол № 8.

Заместитель генерального директора
по науке и развитию АО «НИИ ПС»,
доктор технических наук, профессор

Езерский
Владимир Васильевич

Руководитель центра компетенции СПО АО «НИИ ПС»,
кандидат физико-математических наук, доцент

Хахаев
Иван Анатольевич