УТВЕРЖДАЮ

Заместитель директора по научной работе

ФГУ ФНЦ НИИСИ РАН,

директор МСЦ РАН - филиала

ФГУ ФНЦ НИИСИ РАН

к.т.н., доцент

Шабанов Борис Михайлович

5 декабря 2017 года

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

Межведомственный суперкомпьютерный центр Российской академии наук - филиал Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук»
(МСЦ РАН - филиал ФГУ ФНЦ НИИСИ РАН)

на диссертационную работу Фурсовой Натальи Игоревны

«Методы мониторинга объектов операционной системы, выполняющейся в виртуальной машине»,

представленную на соискание ученой степени кандидата технических наук по специальности
05.13.11 — «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Диссертация Фурсовой Натальи Игоревны посвящена исследованию проблемы мониторинга объектов операционных систем. Информация, получаемая с помощью методов, является важной для анализа бинарного кода, а для некоторых его видов необходимой.

Актуальность

Целью анализа компьютерных программ является выявление представляющих интерес свойств. Динамический анализ применяется тогда, когда эти свойства можно выявить только во время исполнения анализируемой программы. Для исключения возможных рисков динамический анализ часто проводят в виртуальной машине. Исходным представлением для анализа

является поток инструкций, выполняемый виртуальной машиной. Для эффективного анализа хотелось бы отображать свойства программы в более выразительных, чем поток инструкций, структурах. Например, таких как файлы, процессы, модули, функции.

Для представления свойств на уровне структур и объектов нужны автоматические средства анализа. Существует большое количество средств, позволяющих провести мониторинг программ и выделить структуры. Однако, существующие системы обладают особенностями, например, используют программы агенты. Задачей агентов является сбор данных об исследуемой системе. Данные, полученные с помощью агентов, становятся набором параметров, необходимым для проведения анализа. Проблемами являются трудоемкость написания агента, его загрузка в исследуемую систему (если речь идет о встроенных системах), а также необходимость получения для каждой версии каждой операционной системы своего набора параметров. Не имея нужного набора параметров или возможности загрузки агента в систему, выполнить анализ не получится.

Фурсова Наталья Игоревна в своей диссертационной работе предлагает метод мониторинга объектов операционных систем: файлов, процессов, модулей, функций. В основе метода заложен принцип использования двоичного интерфейса приложений (ABI), он работает без агентов, не требует глубоких знаний о системе, подготовленный набор параметров применим к семействам операционных систем. Метод может быть использован для анализа встроенных систем. Таким образом, опираясь на рассуждения, приведенные выше, можно сделать вывод о том, что проблематика, заявленная в качестве темы научного исследования, является в достаточной степени актуальной.

Общая характеристика диссертационной работы

Диссертация имеет общий объем 120 страниц и состоит из введения, пяти глав, заключения, списков литературы, рисунков и таблиц и приложения.

Во введении обоснована актуальность выбранной темы диссертации, сформулированы цели и задачи исследования, указана научная новизна результатов исследования, раскрыта их научная и практическая значимость и перечислены положения, выносимые на защиту.

В первой главе представлен обзор существующих методов и инструментов, реализующих эти методы. Рассмотрены сильные и слабые стороны методов мониторинга объектов операционных систем. Представлена классификация методов и таблица, отражающая основные особенности методов

и инструментов. Выявлены ограничения и недостатки существующих методов. На основе анализа сделан вывод об отсутствии инструмента, имеющего возможность работать со встроенными системами, не использовать агентов и не требующего глубокого знания устройства анализируемой системы.

Во второй главе автор предлагает модель исследуемой операционной системы. Выделены и описаны сущности, составляющие модель, их атрибуты и операции. Также описан поток данных, предоставляющий информацию о каждой сущности.

В третьей главе предложены два метода: метод мониторинга событий виртуальной машины для получения данных об этих объектах и метод вызова системных функций по запросу анализатора для получения заданных атрибутов объектов. Первый метод является основным в диссертационной работе. Метод является безагентным, требует для работы небольшое количество входных данных, имеющихся в открытом доступе (ABI, форматы динамических библиотек и т.д.). Благодаря этому он применим для анализа встроенных систем и позволяет анализировать системы из одного семейства с одним набором параметров. Второй метод является вспомогательным механизмом, позволяющим получить атрибуты объектов путем встраивания системных вызовов в поток инструкций, выполняющихся эмулятором.

В четвертой главе описана практическая реализация метода мониторинга событий виртуальной машины для получения информации об объектах гостевой операционной системы для операционных систем Windows, Linux и FreeBSD. Инструмент представляет собой набор плагинов для эмулятора QEMU. Плагины позволяют получать информацию о файлах и файловых операциях, процессах, вызываемых библиотечных функциях. Получение всех этих данных расписано на примерах для каждой ОС.

Пятая глава посвящена оценке разработанного инструмента. Представлены результаты функционального тестирования, тестирования производительности, приведено сравнение настроечных параметров с инструментом DECAF.

В заключении перечислены основные результаты работы.

Список литературы включает 54 наименования.

Результаты, полученные в диссертационной работе, соответствуют поставленным целям и сформулированным задачам. Оформление текста диссертации выполнено в соответствии с требованиями, предъявляемыми к диссертационной работе.

Автореферат диссертации излишне подробен, но в целом адекватно

отражает ее содержание.

Научные результаты

Основными научными результатами диссертационной работы Фурсовой Натальи Игоревны являются:

1. Метод мониторинга событий виртуальной машины для получения информации об объектах гостевой операционной системы без внедрения инструментального кода на уровне исследуемой системы.

2. Метод вызова системных функций по запросу анализатора для получения заданных атрибутов объектов операционной системы.

Новизна полученных результатов подтверждается сравнением с результатами известных работ по тематике диссертационного исследования.

Значимость результатов исследования

Разработанные автором методы имеют ценность для разработчиков инструментов динамического анализа, для работы которых необходима высокоуровневая информация, в частности, поведенческий анализ, анализ помеченных данных. Помимо этого, методы могут использоваться для анализа встроенных систем, поскольку не используют агентов, обеспечивают совместимость на уровне семейства ОС и не требуют глубоких знаний о системе.

Практическая ценность

Реализация методов мониторинга объектов операционных систем, представленная в диссертационной работе в виде набора плагинов для эмулятора с открытым исходным кодом QEMU, позволила анализировать ОС встроенных систем, повысить производительность анализа, а также облегчить разработку инструмента для новых операционных систем.

Рекомендации по использованию результатов диссертации

Результаты диссертационной работы Фурсовой Натальи Игоревны могут использоваться не только в качестве входных данных для некоторых видов анализа бинарного кода, но и как самостоятельный инструмент для анализа встроенных систем и систем общего назначения.

Достоверность результатов

Достоверность полученных результатов обеспечивается

непротиворечивостью теоретических выводов и результатов решения практических задач, а также подтверждается экспериментальными данными, представленными в диссертационной работе.

Основные положения диссертации полно отражены в 7 печатных изданиях, 6 из них опубликованы в изданиях перечня ВАК РФ, 2 в индексируемых международными базами данных. Из 7 работ 2 опубликованы автором лично и 5 в соавторстве. Результаты, полученные в ходе диссертационного исследования, прошли апробацию на российских и международных научно-технических конференциях и семинарах.

Замечания

1. Первая глава, посвященная обзору существующих методов и инструментов, занимает почти треть содержательного объема диссертации и могла быть ощутимо сокращена без потери в качестве работы.

2. Для предложенной модели исследуемой системы не приводятся границы применимости. Модель хорошо описывает ОС общего назначения, но упоминаемые в работе встраиваемые системы могут управляться ОС реального времени, для которых отдельные компоненты модели будут неопределенны.

3. Практическая реализация методов выполнена для трех операционных систем (Winsows, Linux, FreeBSD), но для ОС FreeBSD представлено описание только для отслеживания файловых операций.

4. Текст диссертации содержит стилистические погрешности, мешающие пониманию сути работы.

Заключение

Приведенные выше недостатки не влияют на общую положительную оценку диссертации. Результаты диссертационной работы Фурсовой Н.И. обладают научной новизной и практической полезностью, а сама работа может быть квалифицирована как завершенное научное исследование по актуальной теме.

Основные результаты диссертации опубликованы в открытой печати: в статьях в изданиях, включенных в список ВАК, в трудах ряда российских и международных конференций. Автореферат диссертации в полной мере раскрывает содержание представленной работы.

Тексты диссертации и автореферата написаны в научном стиле и надлежащим образом оформлены.

Таким образом, диссертация Фурсовой Натальи Игоревны является

законченной научно-исследовательской работой и удовлетворяет всем требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а ее автор, Фурсова Наталья Игоревна, заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных систем.

Отзыв на диссертацию обсужден на научном семинаре Межведомственного суперкомпьютерного центра Российской академии наук - филиала Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» 4 декабря 2017 года, протокол № 13.

заместитель директора МСЦ РАН - филиала ФГУ ФНЦ НИИСИ РАН к.т.н., доцент — Баранов Антон Викторович

ведущий научный сотрудник МСЦ РАН - филиала ФГУ ФНЦ НИИСИ РАН к.ф.-м.н. — Рыбаков Алексей Анатольевич