ОТЗЫВ
ОФИЦИАЛЬНОГО ОППОНЕНТА
на диссертационную работу Фурсовой Натальи Игоревны «Методы мониторинга объектов операционной системы, выполняющейся в виртуальной машине», представленную к защите на соискание ученой степени кандидата технических наук по специальности 05.13.11 - «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Диссертационная работа Н.И. Фурсовой посвящена исследованию и разработке новых методов мониторинга объектов операционных систем (файлов, процессов, модулей, вызываемых функций). Новизна подхода, развиваемого диссертантом, связана с отказом от использования метода программных агентов – метода, который является основным в настоящее время. Этот метод предполагает загрузку программ-агентов в систему для сбора данных о структурах, адресах функций и других данных. Однако, это часто невозможно в случае систем с закрытым исходным кодом, или систем, не предусматривающих загрузку внешних программ. В своей диссертации Н.И. Фурсова рассматривает проблему мониторинга объектов операционной системы, выполняющейся в виртуальной машине. Отметим актуальность такой постановки задачи, так как использование встроенных систем в виртуальной среде является одним из важнейших трендов на современном этапе развития информационных технологий.

В диссертационной работе Фурсова Н.И. предлагает новый метод мониторинга, предполагающий использовать данные о системе, находящиеся в свободном доступе и не привязанные к конкретной версии исследуемой операционной системы. Метод позволяет анализировать встроенные системы, при этом один и тот же набор параметров используется для всего семейства исследуемой операционной системы. Цель диссертационной работы – разработка методов и программных инструментов (плагинов к эмулятору), реализующих мониторинг гостевой ОС (работающей в виртуальной среде) при ее выполнении в программном эмуляторе. Такой подход обеспечивает работу анализатора для всех версий и вариантов ОС данного семейства без внесения изменений в алгоритмы анализа. При этом получение заданных атрибутов объектов ОС происходит по запросу анализатора через встраивание вызовов системных функций в поток инструкций виртуальной машины. В этом мы также видим новизну подхода, развиваемого Н.И. Фурсовой.

Разработанные в диссертации методы имеют четкую прикладную значимость для разработчиков новых инструментов динамического анализа встроенных систем, в том числе и в прикладных исследованиях по информационной безопасности на основе анализа поведения исполняемого ПО.

Отметим, что результаты, полученные в диссертационной работе Н.И. Фурсовой, являются научно обоснованными, что обеспечивается использованием методов динамического анализа и обратной инженерии бинарного кода, системного анализа и метода математического моделирования.

Диссертация содержит 120 страниц, она включает Введение, пять глав, Заключение, списков литературы (54 источника), рисунков (10 рисунков) и таблиц (9 таблиц), и Приложения.

Во Введении обосновывается актуальность темы, формулируются цели и задачи исследования.

Первая глава посвящена обзору существующих методов и средств мониторинга объектов операционных систем, выполняющихся в виртуальной машине.

Во второй главе строится модель исследуемой операционной системы, включая набор сущностей, информацию о которых требуется получить в процессе мониторинга, и источник информации.

Третья глава посвящена описанию разработанных в диссертации методов. Основным из этих методов является метод мониторинга событий виртуальной машины для получения информации об объектах ОС. Он разработан с использованием двоичного интерфейса приложений без использования программ-агентов, тем самым, не затрагивая структуры ядра исследуемой ОС. Получение данных происходит по модели, описанной во второй главе. Также описывается метод дополнения этих данных, необходимых для встраивания вызовов системных функций в поток выполнения эмулятора, восстанавливая таким образом недостающие характеристики объектов. Приводятся ограничения предлагаемого метода мониторинга событий виртуальной машины.

В четвертой главе описана реализация инструментальной среды, разработанной на основе предложенного метода мониторинга событий виртуальной машины. Разработанный инструмент представляет собой набор плагинов для эмулятора QEMU. Представлены наборы для семейств операционных систем Windows, Linux и FreeBSD.

В пятой главе представлены оценка разработанного инструментария по производительности (в сравнении с системой DECAF), проверка достоверности результатов и сравнение сложности настройки разработанного инструмента в сравнении с той же платформой DECAF.

В Заключении перечисляются основные результаты работы.

В Приложении приведены конфигурационные файлы инструментария DECAF.

Перечислим основные результаты, полученные Фурсовой Н.И. в ходе выполнения диссертационного исследования:

- разработка нового метода мониторинга событий виртуальной машины для получения информации об объектах гостевой операционной системы без внедрения инструментального кода на уровне исследуемой ОС;
- разработка метода вызова системных функций по запросу анализатора для получения заданных атрибутов объектов ОС.

Отметим, что разработанная инструментальная среда может функционировать с тремя основными семействами операционных систем общего назначения (Windows, Linux и FreeBSD).

Результаты, выносимые диссертантом на защиту, опубликованы в пяти статьях в рецензируемых журналах, рекомендованных ВАК, один из которых индексируется Scopus, а также в двух публикациях в трудах международных научных конференций, которые также индексируются Scopus.

Достоверность научных положений и выводов диссертационной работы Н.И. Фурсовой обоснована корректностью постановки решаемых задач, использованием современных математических и ИТ методов, а также проверкой валидности данных, получаемых с помощью разработанных методов и инструментов с помощью утилит, доверие к которым не вызывает сомнений (утилиты «Диспетчер задач» для семейства ОС Windows, и утилиты «strace» для ОС Linux).

В заключение отметим, что представленная диссертация Н.И. Фурсовой представляет собой завершенное исследование, проведенное на высоком научно-техническом уровне. Основное содержание диссертации отражено в опубликованных диссертантом статьях и доложено на научных конференциях. Полученные результаты диссертационной работы соответствуют поставленным задачам. Автореферат отражает основные положения диссертации.

Приходим к заключению, что диссертационная работа Фурсовой Натальи Игоревны по теме «Методы мониторинга объектов операционной системы,

выполняющейся в виртуальной машине» соответствует всем требованиям ВАК РФ, предъявляемых к диссертациям на соискание учёной степени кандидата технических наук, а её 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 сетей».

Официальный оппонент:

Доктор физико-математических наук,
начальник Отдела информационных технологий
и математического моделирования
Курчатовского комплекса НБИКС-технологий
НИЦ «Курчатовский институт»
123182 Россия, Москва,
пл. Академика Курчатова, д. 1
тел. +7 915 016-00-48
e-mail: ilyin0048@gmail.com

В.А. Ильин
04.12.2017

Подпись сотрудника НИЦ «Курчатовский институт» В.А. Ильина заверяю

Директор департамента
по общим кадровым и социальным вопросам
НИЦ «Курчатовский институт» С.В. Андрущук