Экз. № 1

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

Козачка Александра Васильевича
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»

Актуальность

Исследование программного обеспечения является и будет являться актуальной задачей еще долгое время. Этой теме и посвящена диссертационная работа Фурсовой Натальи Игоревны.

Анализ предлагается проводить в виртуальной машине, что является удобным и безопасным способом. Однако, это влечет за собой особенность, названную семантическим зазором, другими словами это отсутствие у виртуальной машины данных необходимого уровня для проведения анализа.

Решить проблему семантического зазора можно с помощью мониторинга объектов операционных систем. В процессе мониторинга из потока инструкций виртуальной машины можно получать высокоуровневую информацию, необходимую для анализа. Существующие инструменты, по большей части, используют для этого программы-агенты, которые вынуждены обращаться к структурам ядра операционной системы. В связи с этим разработка и поддержка таких инструментов является трудоемкой задачей, кроме того, такой подход вынужден подстраивать параметры для каждой версии каждой операционной системы и не применим к анализу встроенных систем.

Фурсова Наталья Игоревна в своей диссертационной работе предлагает метод мониторинга объектов операционных систем, основанный на использовании двоичного интерфейса приложений (ABI). Метод разработан таким образом, что не требует глубоких знаний о системе, подготовленный набор параметров применим к семействам операционных систем, также он может быть использован для анализа встроенных систем. Все вышеперечисленное определяет актуальность этой работы.

Достоверность и обоснованность результатов

Диссертация содержит 120 страниц и состоит из введения, пяти глав,

заключения, списков рисунков, таблиц, литературы и приложений. Список литературы содержит 54 наименования.

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

В первой главе представлен обзор современных методов и средств мониторинга объектов операционных систем (ОС), выполняющихся в виртуальной машине. Представлены плюсы и минусы рассмотренных методов и средств и делается вывод о необходимости развития методов, позволяющих анализировать встроенные системы, семейства ОС, не обладая при этом глубокими знаниями о системе.

Во второй главе определена и описана модель исследуемой операционной системы. Выделены объекты, подвергаемые исследованию, описаны их характеристики и операции, а также определены связи между объектами.

В третьей главе представлено описание предлагаемых автором методов. Метод мониторинга событий виртуальной машины для получения информации об объектах ОС является основным результатом диссертации. Он предполагает исследование системы без использования программы-агента и не затрагивает структуры ядра исследуемой ОС. Для разработки метода автор использует данные, предоставляемые в основном двоичным интерфейсом приложений, который предоставлен в открытом доступе для большинства систем. В главе описано каким образом можно получать данные, согласно модели, описанной во второй главе. Второй метод является вспомогательным для вышеописанного. Он позволяет встраивать вызовы системных функций в поток выполнения эмулятора, восстанавливая таким образом недостающие характеристики объектов. В выводах по главе определены ограничения предлагаемого метода мониторинга событий виртуальной машины.

В четвертой главе описана практическая реализация метода мониторинга событий виртуальной машины. Разработанный инструмент представляет собой набор плагинов для эмулятора QEMU. Представлены наборы для операционных систем Windows, Linux и FreeBSD.

Пятая глава посвящена оценке разработанного инструмента. Представлены результаты оценки производительности по сравнению с другими системами, оценка достоверности результатов и сравнение настройки разработанного инструмента с платформой DECAF.

В заключении перечисляются основные результаты работы.

Достоверность научных положений, сформулированных в диссертации, подтверждается практическими разработками, проводимыми в ИСП РАН.

Научная новизна исследования

Научной новизной обладают следующие выносимые на защиту результаты, полученные лично автором в ходе диссертационного исследования:

1. Предложенный автором метод получения информации об объектах ОС через мониторинг событий виртуальной машины, позволяющий анализировать встроенные системы, а также семейства ОС.

2. Метод получения заданных атрибутов объектов ОС по запросу анализатора через встраивание вызовов системных функций в поток инструкций виртуальной машины.

Практическая ценность диссертации

Инструмент, разработанный автором на основе предложенных методов, представляет собой набор плагинов для эмулятора QEMU. Практическая значимость диссертации подтверждается успешным использованием разработанного автором инструмента для осуществления анализа встроенных систем, анализа помеченных данных и поведения программ.

Основные результаты диссертации

Все основные положения диссертации достаточно полно изложены в 7 научных публикациях автора, прошли апробацию на различных научно-технических конференциях (в том числе и зарубежных) и семинарах. Изданные по теме работы публикации характеризуют значительный личный вклад автора в развитие методов мониторинга объектов операционных систем.

Диссертация соответствует специальности 05.13.11 - Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Недостатки и критические замечания

1. В первой главе диссертации (с. 43) представлена таблица, отражающая результаты сравнения разработанного подхода с существующими. Она также представлена в автореферате на с. 9, но в сокращенном варианте, где из-за отсутствия некоторых ключевых критериев преимущества предлагаемого метода становятся не очевидными.

2. В диссертации на рисунке 2.2 "Схема потоков данных" (с. 52) не вполне понятно назначение и способ использования некоторых блоков (память, вызов

API функции).

3. К тексту диссертации имеются претензии в плане стилистики.

Выводы

Диссертация Фурсовой Натальи Игоревны является оригинальной и законченной научно-исследовательской работой, имеющей существенное значение в области исследования поведения программ.

Полученные результаты работы отвечают поставленным в ней задачам, содержание автореферата соответствует основным положениям диссертации.

Диссертационная работа отвечает всем требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, а 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:
кандидат технических наук,
сотрудник Федерального государственного казенного военного
образовательного учреждения высшего образования
«Академия Федеральной службы охраны Российской Федерации»

Козачок А. В.

"1" декабря 2017 г.

Подпись кандидата технических наук Козачка Александра Васильевича заверяю.

Руководитель кадрового ап

Дёшин А. И.

"07" декабря 2017 г.