

Рецензия
на дипломную работу студента МФТИ (ГУ),
919 группы ФРТК, Перова М.Н. на тему
«Разработка кроссплатформенного динамического анализатора
бинарного кода на основе QEMU»

Дипломная работа Перова М.Н. относится к области разработки средств анализа бинарных файлов. Инструмент, предложенный в работе, позволяет анализировать бинарные файлы, как самых распространенных архитектур, так и более редких. Более того, в данный инструмент можно встраивать новые архитектуры в полуавтоматизированном режиме.

Дипломная работа содержит все необходимые структурные компоненты, такие как: введение, пять глав, заключение, список используемой литературы, а также одно приложение.

Материал работы изложен с соблюдением внутренней логики, между разделами прослеживается логическая взаимосвязь. Во введении Максим Николаевич убедительно доказывает актуальность своего исследования, грамотно ставит цели и задачи.

В первой главе рассмотрены статические и динамические методы анализа кода, а также детально изучена технология DBI. Во второй главе проведен обзор существующих средств динамической бинарной инструментации. В третьей главе детально изучен эмулятор QEMU, на основе которого реализован кроссплатформенный динамический анализатор бинарного кода. В четвертой главе предложен способ полуавтоматизированного встраивания новой архитектуры в эмулятор

QEMU, а следовательно и в созданный инструмент. В пятой главе рассмотрен способ идентификации переполнения буфера в стеке, а также его реализация в кроссплатформенном динамическом анализаторе бинарного кода. В приложении приведён исходный код программы, уязвимой к переполнению буфера в стеке.

В целом тема диплома рассмотрена полно, ее результаты внедрены в решения компании «РЕДА-Софт» и применяются в разработках лаборатории 5ТОП100 «Лаборатория моделирования и проектирования архитектур специальных вычислительных систем» МФТИ (ГУ). Существенных недостатков в работе не выявлено. Считаю, что дипломная работа выполнена на высоком техническом уровне и заслуживает оценки «отлично», а Перов М.Н. – присвоения квалификации «математик» по специальности «Компьютерная безопасность» и рекомендации к поступлению в аспирантуру.

Рецензент:

Фонин Юрий Николаевич

05 февраля 2015 г.