Применение технологий виртуализации в процессе фаззинга программных компонентов

Велижанин Анатолий Сергеевич
Тюменский государственный нефтегазовый университет (Тюмень), Россия
e-mail: Anatoliy.Velizhanin@gmail.com

Ревнивых А. В.

В работе рассматривается фаззинг оперативной памяти. Данный подход основывается на внедрении потенциально опасных данных, предположительно способных вызвать сбои в работе программного модуля, в адресное пространство исследуемого процесса. Рассмотрены основные недостатки подходов MLI [1] и SRM [1] для задачи тестирования современных Native (скомпилированного в машинный код текущей аппаратной платформы) программных решений, Managed (построенных для платформы Microsoft .NET Framework) управляемых модулей и Mixed (сочетающих в себе не только Managed, но и Native программный код) решений. В работе предложен вариант решения проблемы фаззинга адресного пространства современных программных решений основанный на применении технологии виртуализации. Данное решение позволяет не только проводить тестирование Managed и Mixed систем, но и уменьшает степень влияния внешних объектов на исследуемый процесс, что улучшает качество тестирования Native систем. В то же время данный подход является ресурсоемким.

Список литературы

[1] Саттон М., Грин А., Амини П. Fuzzing. Исследование уязвимостей методом грубой силы. / Символ-Плюс, 2009.