Разработка средства проверки корректности адресов возврата на платформе S^2E

Евард Вадим <v.e.evard@gmail.com>
345 группа

СПбГУ

Руководитель:
Илья Валерьевич Зеленчук, УрФУ

31 мая 2012

Задача

Разработать инструмент для обнаружения перезаписи адресов возврата в аппаратном стеке

Мотивация:

- обнаружение, облегчение исправления ошибок
- упрощение эксплуатации уязвимости
- доказательство защищённости от данной уязвимости

Инструмент

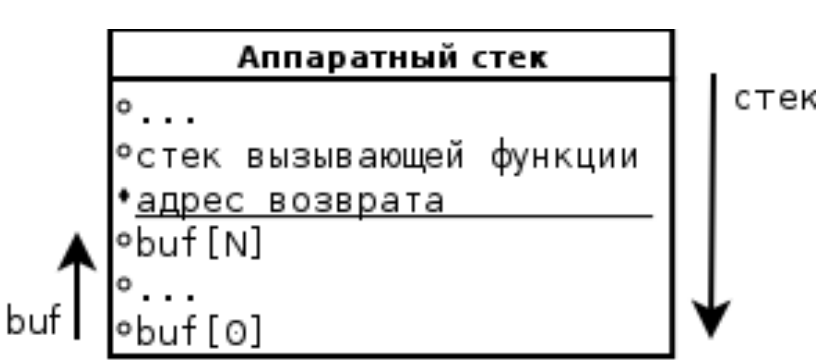
Символьное исполнение -

Интерпретация программы, при которой некоторым переменным приписывается символьное значение

S^2E

Модификация виртуальной машины QEMU для символьного исполнения x86-кода в среде KLEE

Принцип работы



Результат

- реализован модуль к S^2E, проверяющий корректность адресов возврата
- конкретные тестовые данные, приводящие к ошибке, выводятся для простых приложений
- подготовлена среда для тестирования программ, разбирающих сложные форматы данных