УДК 00.004

РАЗРАБОТКА ИНСТРУМЕНТА АНАЛИЗА ДРАЙВЕРОВ WINDOWS НА ОСНОВЕ СИМВОЛЬНОГО ВЫПОЛНЕНИЯ

Читах А.Е. (Университет ИТМО)
Научный руководитель – Ханов А.Р.
(Университет ИТМО)

Аннотация: Целью работы является упрощение и унификация процесса подготовки к исследованию драйверов с помощью фремворка символьного выполнения Angr. Основное содержание исследования посвящено обзору существующих инструментов, реализующих символьное выполнение и разбору принципов работы Angr. Результатом работы является метод, существенно упрощающий процесс подготовки к фаззингу драйверов и программное средство реализующее данный метод.

Введение. Беспрецедентное распространение устройств, подключенных к сети, и рост числа коммуникаций, сложность операционных систем подвергает современную инфраструктуру ИКТ злонамеренным вторжения различных злоумышленников, которые могут украсть конфиденциальную информацию, получить несанкционированный доступ и нарушить работу компьютерных систем. Исходя из того, что драйвера в любой системе обладают наивысшими привилегиями, атака, в которой фигурируют уязвимые или вредоносные драйвера, может нанести колоссальный ущерб системе и привести к утечке конфиденциальных данных. Одним из методов предотвращения атак такого типа является исследование доверенных драйверов на предмет поиска уязвимостей. Наиболее распространённым и универсальным инструментом, позволяющим это осуществить, является фаззинг. Однако, подготовка к фаззингу таких нестандартных объектов как драйвера является достаточно трудоемкой и нетривиальной задачей. На текущий момент не существует универсального решения, которое позволяет упростить и автоматизировать подготовку к фаззингу драйверов.

Основная часть. В данной работе в качестве решения задачи упрощения процесса подготовки к фаззингу драйверов выступает программное средство, реализованное на языке Python с использованием фреймворка символьного выполнения Angr.

Выводы. Результаты данного исследования могут выступать в качестве практической основы для дальнейшей автоматизации подготовки к фаззингу драйверов, а также имеют ценность как фактическое применение символьного выполнения для целей, не ограничивающихся использованием данного фреймворка для решения одноразовых задач, таких как подбор пароля или лицензионного ключа.

Читах А.Е. (автор) Подпись

Ханов А.Р. (научный руководитель) Подпись