Автоматизация создания снимков системы для фаззинга Windows–приложений

Парфенов Илья Дмитриевич,
Новиков Александр Андреевич, Попов Максим Денисович
Студент
Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия
E-mail: parfenov@ispras.ru

Научный руководитель *— Курмангалеев Шамиль Фаимович*

Повсеместное использование программного обеспечения несет определенные риски – каждый год в нем обнаруживаются тысячи новых ошибок. В связи с этим необходимо развивать методы поиска таких дефектов. Один из зарекомендовавших себя методов обнаружения ошибок – это фаззинг. Фаззинг – один из методов динамического анализа ПО, при котором на вход программе подаются неожиданные или специальным образом сгенерированные данные с целью вызвать аварийное завершение программы. Анализ сложных систем является ресурсоемким процессом как по времени, так и по вычислительной мощности, поэтому актуальной задачей является ускорение фаззинга с помощью применения снимков памяти. Это позволяет быстро переключаться между состояниями программы. В частности, появляется возможность производить фаззинг отдельных компонент системы, как, например, сделано в фаззере Nyx [1], где применяются полносистемные снимки памяти. Это также полезно, например, для проведения фаззинга протоколов, где взаимодействуют два приложения, что реализовано, например, в фаззере FitM [2]. Имея доступ к состояниям обоих процессов, легче определить ошибки и причины их возникновения. Однако, существующие фаззеры Windows-приложений с использованием снимков памяти требуют больших трудозатрат на их подготовку. Также, сильно усложнена работа с библиотеками, которые загружаются при выполнении программы (Dynamically Loaded Libraries), так как точки останова нужно ставить в нескольких программах. Зачастую, создание снимков памяти в глубоких состояниях программы является нетривиальной задачей. Например, адреса в программе может быть недостаточно для снятия снимка памяти, так как интересное состояние может быть достигнуто только после многократного выполнения определенных фрагментов кода. В данной работе предложен метод автоматизации создания снимков памяти для фаззинга Windows-приложений. На этапе подготовки к фаззингу происходит

тестовый запуск программы, при котором выделяются интересные состояния на основе информации о системных вызовах, в результате чего получается множество снимков программы в различных состояниях. Далее выполняется фаззинг независимо для каждого из полученных состояний. Разработанный метод был апробирован на системе Windows 11 на ряде приложений без доступа к исходному коду и показал свою жизнеспособность.

Литература

1. S. Schumilo, C. Aschermann, A. Abbasi, S. Worner, and T. Holz, “Nyx: Greybox hypervisor fuzzing using fast snapshots and affine types”, 30th USENIX Security Symposium, 2021. P. 2597–2614
2. Maier D. et al. FitM: binary-only coverage-guided fuzzing for stateful network protocols //Workshop on Binary Analysis Research (BAR). – 2022. – Т. 2022.