Автор:
26.08.14 11:48 -

Разработчики проекта Frida , в рамках которого развивается платформа для динамической трассировки и анализа приложений, предст авили релиз 1.6.3 и новый графический отладчик CryptoShark , основанный на технологиях Frida. По решаемым задачам Frida напоминает DTrace в пространстве пользователя, но для написания скриптов для трассировки и обработки статистики выполнения приложения применяется язык JavaScript. По сути Frida является аналогом Greasemonkey для нативных программ, позволяя контролировать работу программы во время её выполнения также, как Greasemonkey даёт возможность контролировать обработку web-контента.

Трассировка программ поддерживается на платформах Linux, Windows, OS X и iOS. Простейшие сценарии трассировки могут выполняться при помощи утилиты frida-trace (например, "frida-trace -i 'recv*' -i 'read*' Skype"), для более сложных сценариев предлагается подключать обработчики на языке JavaScript. Подобные обработчики имеют полный доступ к памяти процесса, могут перехватывать обращение к функциям и вызывать реализованные в приложении функции из JavaScript-кода. Таким образом в обработчиках может быть организовано двунаправленное взаимодействие с процессом.

Доступность Python-биндинга позволяет использовать язык Python для создания утилит и надстроек над Frida API (скрипты, контролирующие выполнение программы создаются только на JavaScript). Одним из перспективных направлений использования Frida является создание средств для анализа и разбора проприетарных криптографических протоколов и API.

CryptoShark является кроссплатформенной графической надстройкой над Frida, предоставляющей удобный интерфейс для отладки произвольных процессов с использованием техники динамической рекомпиляции. Работа осуществляется на уровне машинного кода, без необходимости наличия отладочной информации или исходных текстов. Поддерживается установка тегов на вызовы API, отображение данных о вызываемых функциях в режиме реального времени, подстановка вызовов для детального журналирования действий.

Базовые компоненты Frida написаны с использованием языков Си и Vala. Для обработки

Автор:
26.08.14 11:48 -

JavaScript применяется движок V8. Отладчик CryptoShark написан на языке C++ и использует для построения интерфейса библиотеку Qt5, а для дизассемблирования - фреймворк Capstone . Исходные тексты всех компонентов проекта распространяются под свободной лицензией
wxWindows Library Licence
(вариант LGPL, не накладывающий ограничений на условия распространения бинарных сборок производных работ).

Read more http://www.opennet.ru/opennews/art.shtml?num=40455