ТЕСТИРОВАНИЕ ИСПОЛНЯЕМЫХ ФАЙЛОВ НА УЯЗВИМОСТИ С ИСПОЛЬЗОВАНИЕМ МЕТОДА SYMBOLIC EXECUTION

А.М. Аблецов

Выявление уязвимостей какой-либо инфраструктуры является одним из ключевых способов для противодействия вредоносной активности, в том числе вредоносному программному обеспечению. Основными методами защиты от эксплуатации уязвимостей исполняемых файлов связанными с менеджментом памяти являются механизмы: предотвращение выполнения данных (DEP), рандомизация размещения адресного пространства (ASLR), позиционно-независимый код (PIC), механизм cannary, ограничение на изменение глобальной таблицы смещения (GOT), замена уязвимых функций на их безопасные аналоги. Так как исполняемые файлы являются одни из основных элементов любой инфраструктуры, то тестирование их на уязвимости ключевая задача для поддержания общего уровня безопасности защищаемой системы.

В настоящее время существует два подхода к тестированию исполняемых файлов на уязвимости: динамический и статический анализ. При динамическом анализе, исполняемый файл тестируется на уязвимости посредством подачи потенциально зловредных входных данных и детектировании аномального поведения программы. Статический анализ предполагает анализ заголовков файлов, инструкций ассемблера, строк данных без непосредственного исполнения тестируемого файла в системе. Одним из ответвлений статического анализа является метод Symbolic Execution. Суть метода Symbolic Execution заключается в том, что все условные переходы и вызовы функции тестируемой программы представляются в виде уравнений, относительно входных данных. И, следовательно, входные данные, приводящие к тому либо иному исходу исполнения программы, будут являться решением системы уравнений, что особенно актуально в программах, реализующих алгоритм выявления уязвимостей.