Методика определения интерфейсов поверхности атаки на примере операционной системы Platform V SberLinux OS Server

Татарчук Иван Александрович, главный ИТ-инженер, Tatarchuk.I.A@sbertech.ru,
АО «Сбербанк-Технологии», 117105, город Москва, Новоданиловская наб., д.10

Определение поверхности атаки является одним из важнейших процессов при сертификации ПО во ФСТЭК России. Поверхность атаки определяется экспертным методом, и от эксперта требуется высокий уровень квалификации и техническая насмотренность, чтобы не только всесторонне исследовать объект оценки, но и минимизировать субъективность анализа получаемых в процессе оценки данных. В случае, если объектом оценки является серверная операционная система, то может потребоваться анализ нескольких тысяч исполняемых файлов и библиотек для полного определения ширины и глубины поверхности атаки.

При сертификации и пересертификации Platform V SberLinux OS Server была разработана методика определения интерфейсов поверхности атаки для ОС. Методика описывает набор конкретных критериев для выделения из многочисленного списка только тех файлов, которые предоставляют злоумышленникам интерфейсы для атаки. Такой подход позволят существенно сократить трудозатраты специалистов и время на определение поверхности атаки для всей операционной системы за счет встроенных механизмов автоматизации.

Определение поверхности атаки для ОС является непрерывным процессом из-за включения в поставку новых пакетов и доработку кода уже существующих. Было предложено разделить процесс на два этапа:

1. выделение программ и библиотек, содержащих код, который может относиться к поверхности атаки
2. уточнение поверхности атаки до конкретных функций в коде программ и библиотек

Второй этап процесса во многих компаниях и лабораториях отлажен в должной мере - для него эксперт использует программные средства анализа помеченных данных на исследовательском стенде и анализирует трассу прохождения данных и поведение программы в контролируемой среде. При этом первый этап процесса описан только в виде общих рекомендаций в «Методике ВУ и НДВ» ФСТЭК РФ.

В докладе описывается процесс определения поверхности атаки по разработанной методике:

- основные положения методики
- принципы отбора бинарных файлов
- выделение критериев определение наличия интерфейсов атаки у бинарного файла
- выявление интерфейсов доступных злоумышленнику
- автоматизация поиска критериев наличия интерфейсов атаки
- рекомендации по анализу результатов полученных после автоматизации
- опыт внедрения методики в сборочный конвейер продукта.

Также проводится анализ результатов внедрения методики в процесс пересертификации продукта. Даются практические рекомендации по обеспечению измерения поверхности атаки вглубь и вширь.

Доклад будет полезен компаниям-разработчикам, которые проводят сертификацию своих ИТ-продуктов, как пример оптимизации определения поверхности атаки.