УДК 004.052.32

РАЗРАБОТКА КОМПЛЕКСА ПРОГРАММНО-ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ ДЛЯ АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ AMD PLATFORM SECURITY PROCESSOR НА НАЛИЧИЕ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ И УЯЗВИМОСТЕЙ

Смирнова П.О. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Гирик А.В.
(Университет ИТМО)

В работе представлен анализ безопасности программного обеспечения процессоров компании AMD, в частности его подсистемы AMD Platform Security Processor (PSP). Рассмотрены принципы работы процессоров, структура хранения программного обеспечения. Предложены алгоритмы извлечения программного обеспечения и алгоритмы детектирования уязвимостей, на основе которых разработан комплекс программно-инструментальных средств для анализа программного обеспечения AMD PSP.

Введение. Процессоры компании AMD в последнее время становятся популярнее, и многие пользователи переходят на их использование. Однако, тот факт, что ранее исследованием безопасности этих процессоров занимались менее значительно, приводит к тому, что отсутствует инструментарий для проведения работ такого типа. Программное обеспечение AMD PSP исполняется первым при запуске электронно-вычислительной машины, имеет наивысшие привилегии, является корнем доверия для всех последующих исполняемых программ, выполняет собственный программный код параллельно с исполнением кода основного процессора, имеет доступ к пространству памяти, в котором работают приложения пользователя, что вызывает опасения по поводу безопасности этой системы. Целостность и отсутствие закладок в подобном продукте являются критичными. Это приводит к тому, что необходим комплекс средств для исследования процессора AMD PSP на наличие недекларированных возможностей и уязвимостей, который бы позволил выделить модули программного обеспечения процессора и исследовать программный код.

Основная часть. Значительной частью данной работы является разработка алгоритмов. Для разработки алгоритма извлечения модулей программного обеспечения были проанализированы программный код из флеш-памяти на материнских платах и файлы обновления программного обеспечения процессоров. Их структура документирована только частично, значение недокументированной части было распознано как самостоятельно, так и на основании других научных работ. Для разработки алгоритма детектирования уязвимостей были проанализированы записи базы данных уязвимостей Common Vulnerabilities and Exposures (CVE), откуда можно выделить конкретные места и паттерны типовых уязвимостей. Для разработки комплекса программно-инструментальных средств одним из этапов является выбор инструментального средства для анализа программного кода, в которое будет добавлен функционал по извлечению модулей программного обеспечения и детектирования уязвимостей. Были составлены критерии, среди которых: наличие декомпилятора – для удобства анализа кода, кроссплатформенность – для большего охвата аудитории исследователей безопасности. В зависимости от выбранного инструментального средства, определялся язык программирования для реализации описанных выше алгоритмов.

Выводы. Разработанный комплекс программно-инструментальных средств позволяет исследователям безопасности выявлять уязвимости и недекларированные возможности в программном обеспечении AMD PSP более эффективно за счёт работы в инструментальном средстве и извлечения модулей программного обеспечения. Предложенный алгоритм детектирования уязвимостей выявляет заданное подмножество известных уязвимостей.

Смирнова П.О. (автор) Подпись

Гирик А.В. (научный руководитель) Подпись