УДК 004.052.2

ИССЛЕДОВАНИЕ УСТОЙЧИВОСТИ UEFI-СОВМЕСТИМЫХ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ

Захаров О.О., Дудкин А.С. Военно-космическая академия имени А.Ф. Можайского
Научный руководитель – кандидат технических наук Дудкин А.С.
Военно-космическая академия имени А.Ф. Можайского

В докладе представлено направление исследований устойчивости UEFI-совместимых программно-аппаратных комплексов, выдвинуты предложения по улучшению средств защиты информации и политик безопасности.

Введение. Unified Extensible Firmware Interface (UEFI) – интерфейс между операционной системой и микропрограммами, предназначенный для замены устаревшего BIOS. Несмотря на встроенные технологии безопасности, количество атак на UEFI с каждым годом растет, поскольку данный интерфейс представляет особый интерес для злоумышленников из-за его возможностей – запуск кода до загрузки операционной системы, хранение данных в NVRAM, позволяющее избегать средства защиты информации и другие особенности, которые помогают успешно проводить компьютерные атаки.

Основная часть. Прошивка UEFI располагается на SPI (Serial Peripheral Interface) микросхемах. Кроме прошивки, на них располагается хранилище NVRAM (Non-Volatile Random Access Memory), предназначенное для постоянного хранения данных в UEFI-совместимых прошивках. Обычно, для NVRAM переменных выделяют область памяти из SPI микросхемы – в целях сокращения расходов на дополнительные компоненты. Микросхемы для UEFI построены на технологии NOR Flash, средний показатель записи/стирания и повторной записи которых составляет 100000 циклов – по данным производителей этого хватит на 10 лет активного использования без сбоев. Однако, высокая температура (например, на производствах), а также частая работа с NVRAM переменными могут уменьшить ее ресурс, что может привести к серьезным последствиям, например, нарушению технологических процессов на производстве. Не менее важным остается вопрос о заполнении памяти случайными данными и то каким образом это повлияет на скорость загрузки, работы программно-аппаратного комплекса. Автором проведено исследование, направленное на выявление недостатков в обеспечении безопасности UEFI современными средствами защиты информации и политиками безопасности.

Выводы. Проведенное автором исследование и выдвинутые предложения по улучшению безопасности и надежности систем, использующих подсистему UEFI, могут оказать помощь в обеспечении их стабильности и работоспособности.

Захаров О.О. (автор)

Дудкин А.С. (научный руководитель)