УДК 004.451.82

Поддержка алгоритма доверенной загрузки в программе начального старта и ядре ОС «Эльбрус»

С.М. Копылов
АО «МЦСТ»

В настоящее время все чаще находит применение механизм доверенной загрузки (МДЗ), представляющий собой комплекс программно-аппаратных средств, направленный на обеспечение защиты вычислительного комплекса (ВК) от несанкционированного доступа. МДЗ подразумевает невозможность загрузки операционной системы с жесткого диска ВК без прохождения идентификации на этапе начальной загрузки, что позволяет выполнить вход в систему только доверенным лицам.

При включении ВК, не содержащего МДЗ, процессор считывает прошивку из постоянного запоминающего устройства (ПЗУ), записывает ее в оперативную память и передает ей управление. Далее код прошивки инициализирует процессор, оперативную память и контроллер периферийных интерфейсов (КПИ), связывающий периферийные устройства и шины с центральным процессором. Если проверка работоспособности аппаратного обеспечения выполнена успешно, код прошивки начинает поиск ядра ОС на доступных носителях ВК. На следующем этапе код прошивки загружает ядро ОС в оперативную память и передает ему управление.

МДЗ состоит из *USB*-замка[1], расположенного на материнской плате ВК, а также прошивки для ПЗУ. Прошивка включает в себя образ, состоящий из загрузчика (*bootloader*) и дистрибутива *BuildRoot,* использующего сжатое ядро *Linux.*

Легковесный дистрибутив *BuildRoot* был создан путем исключения из состава дистрибутива всех пакетов, кроме набора утилит *busybox*.

Для сжатия ядра *Linux* до необходимых размеров, в конфигурационном файле ядра были сделаны следующие правки:

- включены: поддержка алгоритма сжатия ядра, поддержка прерываний, поддержка системного вызова *kexec*;
- отключены: поддержка аудита, возможность выгрузки модулей, поддержка неравномерной памяти (*NUMA*), поддержка сетевых параметров, поддержка фаервола, поддержка прямого удаленного доступа к памяти, поддержка устаревших драйверов, поддержка температурных сенсоров, поддержка мультимедиа.

При включении ВК, содержащего МДЗ, процессор считывает прошивку из ПЗУ, записывает ее в оперативную память и передает ей управление. Далее код прошивки инициализирует процессор, оперативную память и КПИ, что позволяет проинициализировать *USB*-замок. Затем код прошивки записывает сжатое ядро *Linux* в оперативную память и передает ему управление. Таким образом происходит попадание в командную строку *BuildRoot*. Из командной строки необходимо вызвать программу, отвечающую за работу *USB*-замка. При положительном завершении работы программы *USB*-замка, вход в систему будет возможен с помощью системного вызова *kexec*, позволяющего загрузиться из текущего сжатого ядра в ядро ОС «Эльбрус», которое расположено на одном из носителей ВК, пропуская фазу загрузчика. Запуск *kexec* выполняется с двумя аргументами. Первый аргумент — расположение образа ядра, в которое необходимо загрузится. Второй — командная строка ядра.

Литература

1. *Михеев М.Ю., Семочкина И.Ю., Новиков А.В., Свистунов Б.Л.* Технические средства криптографической защиты // Труды Международного симпозиума «Надежность и качество». 2010. №2.