УДК 004.056.5

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ВИРТУАЛИЗАЦИИ ПРИ ТЕСТИРОВАНИИ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Т.М. Каннер

В статье рассматриваются особенности тестирования программно-аппаратных средств защиты информации (СЗИ) в части применения средств виртуализации и проброса аппаратной компоненты в среду виртуальных машин

Ключевые слова: тестирование, программно-аппаратные СЗИ, средства виртуализации, AMD IOMMU, Intel VT-d

В процессе тестирования программно-аппаратных средств защиты информации (СЗИ) может потребоваться использование средств виртуализации, которые позволили бы выполнить следующие задачи:

1) эмулировать большое количество пользователей, процессов и сеансов подключений;

2) провести тестирование на большом количестве программных платформ – в различных версиях и разрядностях операционной системы (ОС);

3) провести последовательное тестирование на нескольких средствах вычислительной техники (СВТ) с переподключением аппаратной компоненты СЗИ;

4) осуществить тестирование СЗИ, часть функций которого функционируют до старта сессии пользователя в ОС.

Во всех перечисленных случаях использование средств виртуализации для программно-аппаратных СЗИ (в отличие от программных) не может полноценно заменить реальные физические СВТ. Средства виртуализации, с одной стороны, упрощают проблему масштабируемости и позволяют автоматизировать ряд проверок, что невозможно сделать на физических СВТ. С другой стороны, – ухудшают «чистоту» эксперимента и вводят еще один уровень (гипервизор виртуальной среды), на котором могут возникать ошибки, не связанные с функционированием самого СЗИ или аппаратных компонент СВТ.

Помимо этого в среде виртуализации не могут быть полноценно сэмулированы все возможные аппаратные платформы, они могут не соответствовать аналогичным физическим СВТ. В случае работоспособности СЗИ в виртуальной среде нет гарантий его работоспособности на реальном СВТ с аналогичными характеристиками. Также из работоспособности аппаратной компоненты СЗИ, подключенной, например, в интерфейс USB-2.0 среды виртуализации, в общем случае необязательно следует ее корректное функционирование при подключении к интерфейсу USB-2.0 реального СВТ.

Кроме того, некоторые среды виртуализации не позволяют «пробрасывать» в виртуальные машины (ВМ) все существующие интерфейсы подключения аппаратной компоненты СЗИ. При использовании виртуализации меньше всего проблем возникает с программно-аппаратными СЗИ, функционирующими в ОС СВТ и имеющими USB-интерфейс подключения, так как все средства виртуализации поддерживают «проброс» USB-устройств в ВМ и существуют соответствующие драйверы для поддержки виртуальных интерфейсов подключения в ОС ВМ. При использовании сред виртуализации для тестирования встраиваемых программно-аппаратных СЗИ, функционирующих независимо от ОС СВТ, возникают проблемы, например, связанные с возможностью инициации загрузки с СЗИ или перехватом управления до загрузки ОС ВМ.

Рассмотрим применение средств виртуализации в рамках тестирования СЗИ от несанкционированного доступа (НСД) «Аккорд-АМДЗ» [1] (встраиваемого СЗИ, функционирующего независимо от ОС СВТ). СЗИ НСД «Аккорд-АМДЗ» включает

Каннер Татьяна Михайловна – ЗАО «ОКБ САПР», e-mail: tatianash@okbsapr.ru

аппаратную компоненту, реализованную для интерфейсов PCI / PCI-express / Mini PCI-express. Соответственно, для его тестирования с использованием средств виртуализации необходимо «пробрасывать» эту аппаратную компоненту в среду виртуализации. Это возможно сделать при помощи следующих технологий – AMD I/O Virtualization Technology (AMD IOMMU) [2] или Intel Virtualization Technology for Directed I/O (Intel VT-d) [3]. В основе этих технологий лежит применение специального устройства управления памятью ввода-вывода (англ. input/output memory management unit, IOMMU), позволяющего напрямую использовать в ВМ различные периферийные устройства (в том числе и с интерфейсом PCI / PCI-express) через таблицы отображения прерываний и прямого доступа к памяти (англ. Direct Memory Access, DMA). Поддержка интерфейса Mini PCI-express возможна с использованием переходника Mini PCI-express – PCI-express. Для корректной работы технологий AMD IOMMU или Intel VT-d, они должны поддерживаться процессором, материнской платой, системным/внутренним ПО СВТ (BIOS или UEFI) и ОС СВТ (в которой используется средство виртуализации). В случае отсутствия поддержки этих технологий в одном из указанных компонент СВТ, «проброс» PCI / PCI-express в ВМ будет невозможен.

Таким образом, для тестирования любых программно-аппаратных СЗИ с PCI-интерфейсом подключения с помощью средств виртуализации необходимо использовать специализированные СВТ, в которых все компоненты поддерживают технологию AMD IOMMU или Intel VT-d. Для обеспечения возможности «проброса» PCI-устройств в ВМ необходимо также обеспечить поддержку этих технологий в ОС. Например, в ОС Linux и среде виртуализации KVM (Kernel-based Virtual Machine) для «проброса» PCI-устройств в ВМ с помощью технологии Intel VT-d, необходимо использовать ядро ОС со следующими параметрами конфигурации:

1) CONFIG_PCI_STUB – для обеспечения возможности «отвязки» PCI-устройств от драйверов ОС и их «проброса» в среду ВМ;

2) CONFIG_INTEL_IOMMU – для включения поддержки Intel VT-d с использованием таблиц отображения DMA (для трансляции всех обращений к физической памяти из ВМ);

3) CONFIG_IRQ_REMAP – для поддержки отображения прерываний.

В дальнейшем для «проброса» PCI-устройств в среду виртуализации KVM, перед запуском ВМ необходимо сначала «отвязать» устройство от драйвера ОС. Затем требуется «привязать» PCI-устройство к драйверу, который будет использоваться для его «проброса» в среду виртуализации (pci_stub). После этого можно запускать ВМ, передавая в качестве параметра расположение устройства на шине PCI (например, «-device pci-assign, host=03:00.0, id=amdz0», где 03:00.0 – интерфейс, в который подключено PCI-устройство). Пример загрузки и перехвата управления после BIOS ВМ с использованием СЗИ НСД «Аккорд-АМДЗ» приведен на рис. 1.

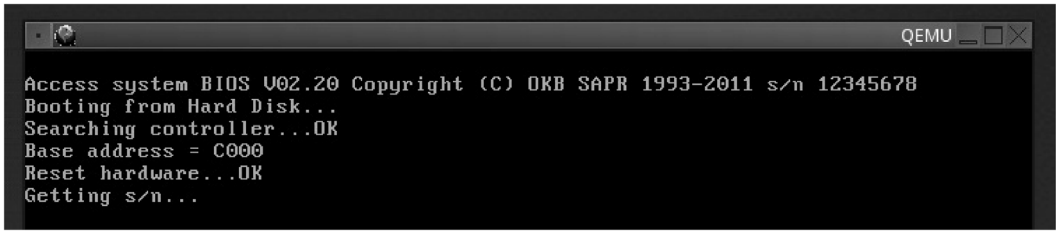

Рис. 1. Загрузка СЗИ НСД «Аккорд-АМДЗ» в виртуальной среде, перехват управления после BIOS ВМ

Для успешного прохождения процедур идентификации/аутентификации СЗИ НСД «Аккорд-АМДЗ» в ВМ (см. рис. 2) необходимо также выполнить «проброс» соответствующего аппаратного идентификатора, в случае необходимости его подключения к USB-порту СВТ (а не к самому СЗИ).

Необходимо отметить, что при таком «пробросе» аппаратной компоненты (PCI-

устройства) СЗИ НСД «Аккорд-АМДЗ» будет контролировать целостность BIOS, программных и «технических» средств ВМ, а не реального СВТ, в котором эта ВМ запущена. Примеры отображения результатов контроля целостности в СЗИ НСД «Аккорд-АМДЗ» и интерфейса формирования списков контроля целостности файловых объектов ВМ изображены на рис. 3 и 4.

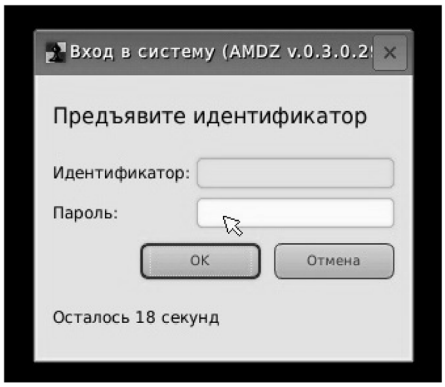

Рис. 2. Процесс идентификации/аутентификации в СЗИ НСД «Аккорд-АМДЗ» в виртуальной среде

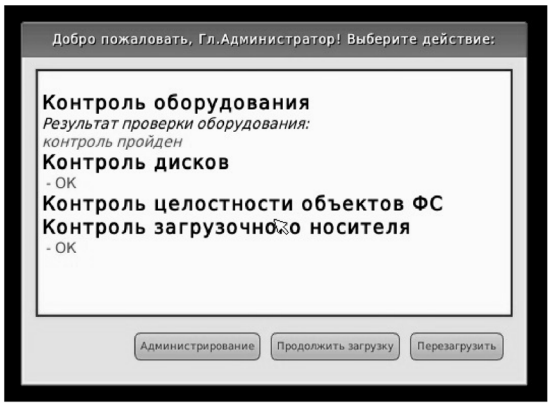

Рис. 3. Отображение результатов контроля целостности программных и «технических» средств ВМ с использованием СЗИ НСД «Аккорд-АМДЗ»

В случае успешного прохождения процедур идентификации/аутентификации и контроля целостности программных и «технических» средств ВМ, управление, как и при работе СЗИ НСД «Аккорд-АМДЗ» на реальном СВТ, передается загрузчику ОС (для Администратора «Аккорд-АМДЗ» доступен выбор источника загрузки).

Таким образом, для использования средств виртуализации в процессе тестирования программно-аппаратных СЗИ, аппаратная компонента которых реализована для интерфейсов PCI / PCI-express / Mini PCI-express (или подобных, более современных интерфейсов на материнской плате СВТ), необходимо применять специализированные СВТ, в которых процессор, материнская плата, системное/внутреннее ПО (BIOS и UEFI) и ОС поддерживают технологии AMD IOMMU или Intel VT-d. При этом для тестирования программно-аппаратных СЗИ, подключаемых к USB-интерфейсу, с помощью средств виртуализации достаточно использовать только их встроенные возможности по «пробросу» USB-устройств. Также необходимо отметить, что СЗИ, функционирующие в среде ОС, в отличие от

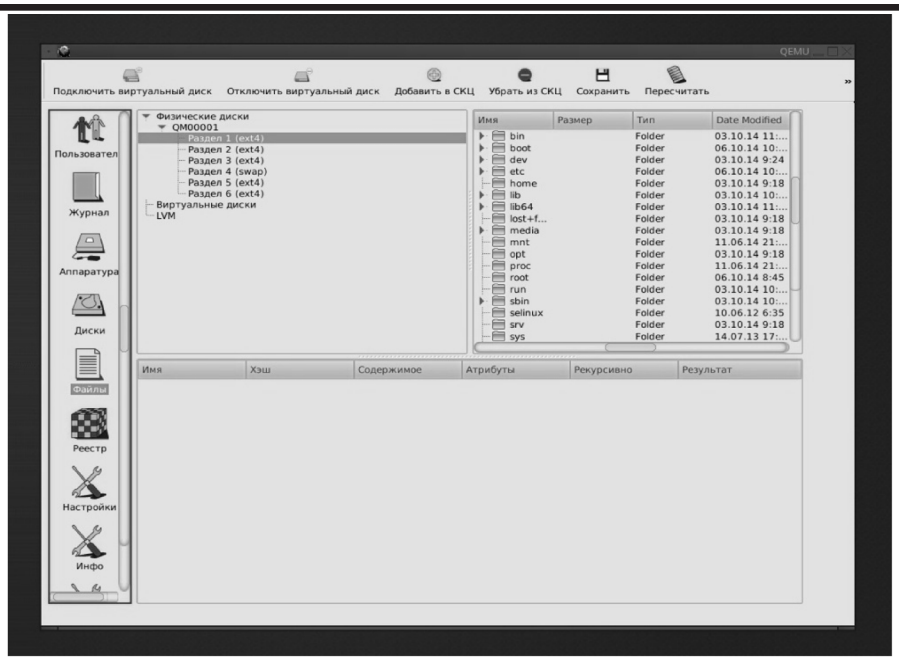

Рис 4. Интерфейс администрирования СЗИ НСД «Аккорд-АМДЗ» при формировании списков контроля целостности файловых объектов ВМ

встраиваемых СЗИ, функционирующих независимо от ОС, имеют меньшую зависимость от аппаратной платформы СВТ [4], на которой производится тестирование. В соответствии с этим для СЗИ, функционирующих в среде ОС, допустимо применение средств виртуализации, так как их использование наименьшим образом будет влиять на результаты тестирования. Для тестирования встраиваемых программно-аппаратных СЗИ, функционирующих независимо от ОС, по возможности необходимо использовать реальные СВТ, что, в свою очередь, усложняет организацию процесса тестирования, но не искажает его результатов.

Литература

1. Программно-аппаратный комплекс средств защиты информации от НСД для ПЭВМ (РС) «Аккорд-АМДЗ». Руководство администратора. 11443195.4012-038 90 2011 // М.: ОКБ САПР. — 2014. — С. 54.

2. AMD I/O Virtualization Technology (IOMMU) Specification Revision 1.26. [Электронный ресурс]. URL: http://developer.amd.com/wordpress/media/2012/10/34434-IOMMU-Rev_1.26_2-11-09.pdf (дата обращения: 19 июня 2015 г.).

3. Intel Virtualization Technology for Directed I/O (VT-d) Architecture Specification. [Электронный ресурс]. URL: http://www.intel.com/content/www/us/en/embedded/technology/virtualization/vt-directed-io-spec.html (дата обращения: 19 июня 2015 г.).

4. Синякин С. А. Особенности совместимости Аккорд-АМДЗ и современных СВТ // Комплексная защита информации. Электроника инфо. Материалы XVIII Международной конференции 21-24 мая 2013 года, Брест (Республика Беларусь). 2013. — № 6. — С. 142–144.

Закрытое акционерное общество «ОКБ САПР»
Closed Joint Stock Company «OKB SAPR»

FEATURES OF USING VIRTUALIZATION FOR TESTING SOFTWARE AND HARDWARE DATA SECURITY TOOLS

T.M. Kanner

The article considers features of testing software and hardware data security tools (DST) in terms of using virtualization and forwarding hardware component in a virtual machine environment

Key words: testing, software and hardware DST, virtualization, AMD IOMMU, Intel VT-d