Мищериков Е.В. Отличие аппаратной виртуализации от программной. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 115-117.

ОТЛИЧИЕ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ ОТ ПРОГРАММНОЙ

Е.В. Мищериков

Пензенский государственный университет,
г. Пенза

Классическая архитектура программной виртуализации подразумевает наличие хостовой операционной системы, поверх которой запускается платформа виртуализации, эмулирующая работу аппаратных компонентов и управляющая аппаратными ресурсами в отношении гостевой операционной системы. Реализация такой платформы достаточно сложна и трудоемка, присутствуют потери производительности в связи с тем, что виртуализация производится поверх хостовой системы. Безопасность виртуальных машин также находится под угрозой, поскольку получение контроля над хостовой операционной системой автоматически означает получение контроля над всеми гостевыми системами.

В отличие от программной техники с помощью аппаратной виртуализации возможно получение изолированных гостевых систем, управляемых гипервизором напрямую. Такой подход может обеспечить простоту реализации платформы виртуализации и увеличить надежность платформы с несколькими одновременно запущенными гостевыми системами, при этом нет потерь производительности на обслуживание хостовой системы. Такая модель позволит приблизить производительность гостевых систем к реальным и сократить затраты производительности на поддержание хостовой платформы.

Стоит также отметить, что аппаратная виртуализация потенциально несет в себе не только положительные моменты. Возможность управления гостевыми системами посредством гипервизора и простота написания платформы виртуализации с использованием аппаратных техник дают возможность разрабатывать вредоносное программное обеспечение, которое после получения контроля над хостовой операционной системой виртуализует ее и осуществляет все действия за ее пределами.

В начале 2006 года был создан руткит под кодовым названием SubVirt, поражающий хостовые системы Windows и Linux и делающий свое присутствие практически необнаруживаемым. Принцип действия этого руткита заключался в следующем:

1. Через одну из уязвимостей в операционной системе компьютера вредоносное программное обеспечение получает административный доступ.

2. После этого руткит начинает процедуру миграции физической платформы на виртуальную, по окончании которой происходит запуск виртуализованной платформы посредством гипервизора. При этом для пользователя ничего не меняется, все продолжает работать, как и раньше, а все средства и службы, необходимые для доступа к гипервизору извне (например, терминального доступа), находятся за пределами виртуализованной системы.

3. Антивирусное программное обеспечение после осуществления процедуры миграции не может обнаружить вредоносный код, поскольку он находится за пределами виртуализованной системы.

Наглядно эта процедура выглядит так:

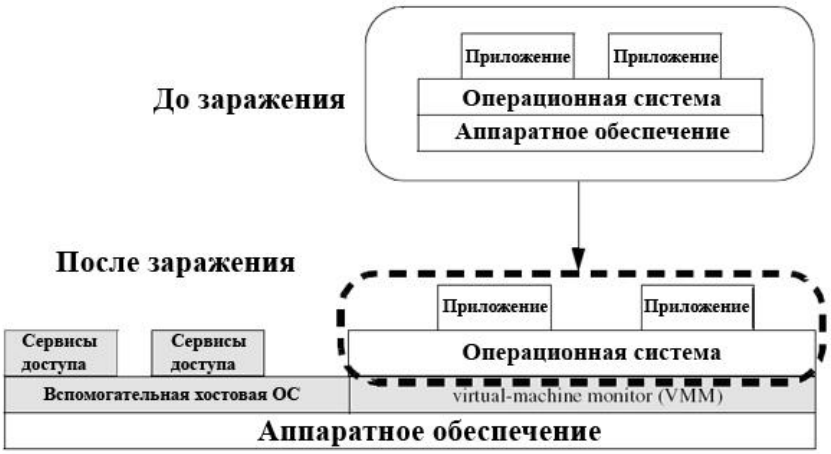

Схема работы руткита

Однако не стоит преувеличивать опасность. Разработать вредоносную программу, использующую технологии виртуализации, гораздо сложнее, нежели пользуясь «традиционными» средствами, эксплуатирующими различные уязвимости в операционных системах. При этом главное допущение, которое делается теми, кто утверждает, что такое вредоносное ПО сложнее в обнаружении и, более того, может не использовать «дырки» в ОС, действуя исключительно «в рамках правил», состоит в том, что, якобы, виртуализованная операционная система не в состоянии обнаружить, что она запущена на виртуальной машине, что есть исходно неверная посылка. Соответственно антивирусное обеспечение имеет все возможности обнаружить факт заражения. А следовательно, пропадает и смысл разрабатывать столь ресурсоемкий и сложный троян, учитывая наличие куда более простых способов вторжения.

Поддержка технологий аппаратной виртуализации в процессорах открывает широкие перспективы по использованию виртуальных машин в качестве надежных, защищенных и гибких инструментов для повышения эффективности виртуальных инфраструктур. Наличие поддержки аппаратных техник виртуализации в процессорах не только серверных, но и настольных систем говорит о серьезности намерений производителей процессоров в отношении всех сегментов рынка пользователей компьютерных систем. Использование аппаратной виртуализации в перспективе должно уменьшить потери производительности при запуске нескольких виртуальных машин на одном физическом сервере. Безусловно, аппаратная виртуализация повысит защищенность виртуальных систем в корпоративных средах. Сейчас простота разработки платформ виртуализации с использованием аппаратных техник привела к появлению новых игроков на рынке средств виртуализации. Вендоры систем паравиртуализации широко применяют аппаратную виртуализацию для запуска немодифицированных гостевых систем. Дополнительным преимуществом аппаратных техник виртуализации является возможность запуска 64-битных гостевых систем на 32-битных версиях платформ виртуализации.