УДК 004.031.43
Т.В. Василенко

Обзор и анализ возможностей виртуальных машин как средства обеспечения безопасности функционирования программных средств

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

Введение

Наиболее уязвимы с точки зрения защищенности информационных ресурсов являются так называемые критические компьютерные системы, угрозы безопасности функционирования которых могут возникать как в процессе создания программного обеспечения для его работы, так и в процессе эксплуатации. Под критическими компьютерными системами (КС) будем понимать сложные компьютеризированные организационно-технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно-транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам [1].

1. Постановка задачи

В настоящее время основные проблемы безопасности техносферы возникают при эксплуатации критических систем, к которым относятся транспортные, энергетические, военно-технические, связные и другие системы. Отказ критической системы класса может привести к значительному экономическому, политическому, моральному и другим ущербам. Безопасность таких систем непосредственным образом зависит от цифровых электронных вычислительных машин со всем их содержимым и в первую очередь от совокупности общих и специальных программных средств создания, обработки и хранения компьютерных данных и собственно компьютеризированных данных. Именно поэтому проблема обеспечения безопасности функционирования систем такого назначения является актуальной.

Зависимость критических систем от технических мер защиты (ТМЗ) порождает необходимость придания применяемым в них программным средствам заданных свойств безопасности и способности противостоять разрушению, нарушениям функционирования системы, сбоям, преднамеренным воздействиям злоумышленников и ошибкам различных видов при выполнении критической системой основной целевой функции. Под ТМЗ понимаются различные электронные устройства и специальные программы, входящие в состав автоматизированной системы, которые выполняют функции защиты информации [2].

Все вышесказанное вынуждает считать проблему обеспечения функциональной безопасности ПО критических систем актуальной и требующей разрешения.

Целью работы является обзор и анализ теоретических возможностей виртуальных машин и их типов, а также возможности их использования как

инструментального средства для обеспечения безопасности функционирования систем критического назначения.

2. Анализ типов виртуальных машин. Архитектура и свойства

Идея виртуализации применима не только к отдельным подсистемам вроде дисков, но и к машине в целом. Для построения виртуальной машины (ВМ) к реальному компьютеру добавляется слой программного обеспечения, поддерживающий желаемую архитектуру. Таким путем можно обойти проблему совместимости реальных машин и ресурсные ограничения оборудования [3].

Существует несколько видов виртуальных машин:

– процессные виртуальные машины, которые создают виртуальные среды ABI (application binary interface) для пользователей и приложений. Различные их разновидности позволяют в многозадачном режиме осуществлять репликацию операционной среды, эмулировать систему команд, оптимизировать код или выполнять программы на языках высокого уровня. Такими машинами являются оптимизаторы двоичного кода, интерпретаторы и динамические трансляторы двоичного кода и т.д. [3]. Одной из простейших процессных машин является сама операционная система. Она предоставляет каждому требующему выполнения процессу отдельное адресное пространство, тем самым осуществляя многозадачность. Таким образом, операционная система предоставляет для каждого выполняемого приложения процессную виртуальную машину;

- системные виртуальные машины, обеспечивающие полнофункциональную среду, в которой могут сосуществовать операционная система и несколько процессов, относящихся к разным пользователям. С помощью системных ВМ одна аппаратная платформа способна одновременно поддерживать несколько изолированных гостевых операционных систем [3]. Большинство системных ВМ обеспечивают примерно одинаковые функциональные возможности, но различаются деталями реализации. Большая часть системных виртуальных машин имеют приблизительно одинаковые возможности, отличие их - лишь в реализации. Например, при классическом подходе [4] монитор устанавливается на аппаратной платформе, а сама виртуальная машина устанавливается поверх него. Если это вложенная виртуальная машина, то она устанавливается поверх на установленную хост-систему. Преимущество таких виртуальных машин состоит в том, что пользователь устанавливает их как обычную программу. Иногда для системных виртуальных машин хостовая и гостевая ОС имеют общую архитектуру систем команд базового оборудования, в таком случае интегральные ВМ виртуализируют операционную систему и все программы.

Одним из важнейших применений технологии системных ВМ является изоляция систем, одновременно работающих на общей аппаратной платформе (в статье речь идет именно о такой ВМ). В таких случаях отказ в работе или нарушение безопасности одной из гостевых систем не влияет на программное обеспечение, выполняющееся на других гостевых системах. Т.е. при помощи одной такой виртуальной машины на одном компьютере можно запустить одновременно как операционную систему (ОС) Windows так и Linux. Такая ситуация положительно отражается на работе по тестированию программного обеспечения, так как нет необходимости устанавливать на одной ЭВМ несколько операционных систем и использовать их постоянно перегружая ЭВМ. Использование виртуальной машины позволяет применять обе ОС посредством

переключения между ними одной операцией. Связи хостовой и гостевых ОС отображены на рисунке.

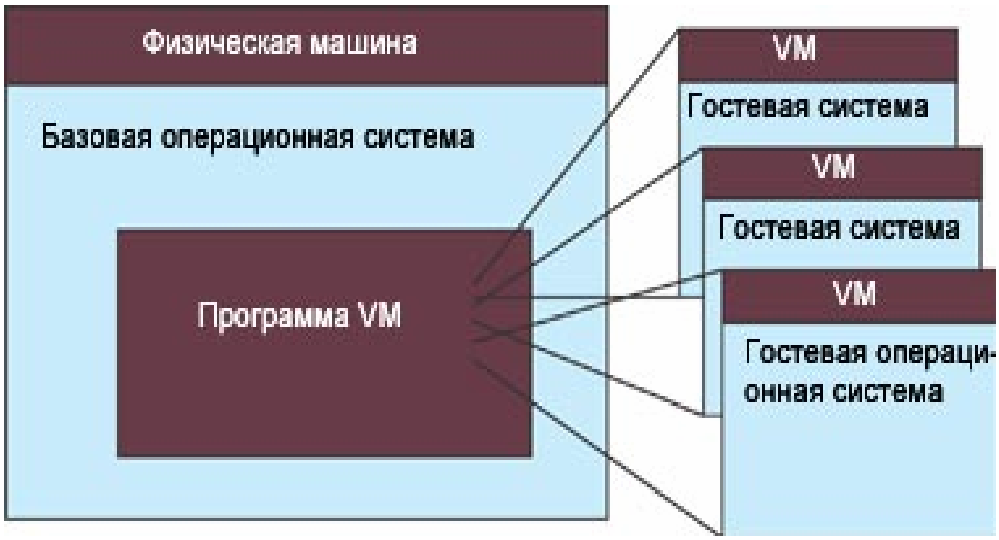

Рис. Связи между хостовой операционной системой и гостевыми ВМ

Ещё одним преимуществом такой машины является возможность демонстрации сетевого взаимодействия между машинами на одном компьютере. Например, продукт VMware Workstation поддерживают четыре типа виртуальных сетевых соединений: None, Host-Only, Bridged и NAT (Network Address Translation — трансляция сетевых адресов) [5], что в свою очередь позволяет говорить о замене шаблона безопасности, использующего аппаратную избыточность на резервирование программными методами.

Виртуальная машина может использовать практически любое оборудование, установленное на компьютере: сетевые карты, порты, звуковые карты, приводы и так далее. Виртуальная машина без проблем переносится между любыми компьютерами с помощью копирования файла конфигурации.

Для полноправной работы любой гостевой операционной системы необходимо выделить ей соответствующий размер ОЗУ, что в материальном смысле намного дешевле приобретения ещё одной аппаратной платформы. Такие же требования следует отнести и к дисковой подсистеме, и к производительности процессора. И даже при этом покупка мощного аппаратного обеспечения для одной ЭВМ и последующая установка виртуальной машины на ней являются более выгодными в финансовом плане, нежели покупка нескольких компьютеров.

У такого решения есть и свой минус – выход из строя любого из аппаратных обеспечений приведет к отказу всей системы. Недостаток окупается повышенной безопасностью работы, простотой развертывания новых платформ и снижением стоимости владения.

3. Обеспечения отказоустойчивости критической системы

Отказоустойчивость, или, другими словами, безопасность технических средств обеспечивается путем резервирования и реконфигурации [6]. Однако это очень трудоемкий и не самый дешевый в финансовом плане процесс. Для обеспечения отказоустойчивости программного обеспечения необходимо иметь

развитые средства обнаружения дефектов, средств ограничения влияния обнаруженной ошибки на работоспособность, а также средств восстановления работоспособности программ после обнаружения ошибки.

Одним из способов обеспечения отказоустойчивости является мягкое резервирование – переход от основного комплекта к резервному, вывод из работы для восстановления работоспособности отказавших модулей, возвращение восстановленных или новых модулей, происходит без нарушения процесса функционирования других работоспособных модулей либо без нарушения других временных ограничений на процесс выполнения программ и подготовки выдаваемых другими модулями информации [6]. В нашем случае предполагается замена резервного аппаратного комплекса программным. Используя специально разработанную модель функционирования, можно воспользоваться заданными возможностями виртуальных машин, в случае обнаружения ошибки.

Выводы

Таким образом, главное преимущество виртуальной машины - это возможность использования общих файлов и приложений за счет взаимодействия по виртуальной сети и запуска различных приложений на одном компьютере под управлением разных операционных систем. Следствием этого является возможность использования системной ВМ как инструментального средства для обеспечения безопасности функционирования системы критического назначения.

Основной идеей данного исследования является попытка оценить эффективность совместного применения виртуальных машин, как инструментальных средств обеспечивающих работу нескольких операционных систем одновременно на одной аппаратной платформе и известных шаблонов проектирования обеспечивающих надежность и функциональную безопасность. При реализации программного обеспечения таких систем могут быть применены различные схемы организации работы многоверсионных программных комплексов.

Список литература

1. Казарин О.В. Безопасность программного обеспечения компьютерных систем. – М:МГУЛ, 2003.-212 с.
2. Лукацкий А.В. Краткий толковый словарь по информационной безопасности. - М, 2000.- 177 с.
3. Смит Дж., Наир Ра. Архитектура виртуальных машин // Открытые системы. - №5-6, 2005.- 40-46 с.
4. R.P. Goldberg, Survey of Virtual Machine Research. // Computer. –1974. - Vol.6.
5. Оти .М. VMware Workstation 4 или Microsoft Virtual PC 2004? // Windows IT Pro. - №4 2004. - 30-34 с.
6. Черкесов Г.Н. Надежность аппаратно-программных комплексов: Учеб. пособ. СПб.: Питер, 2005. - 478 с.