который может послужить в качестве прототипа при реализации системы КОД в среде ОАИС, доступен по адресу [9]. Докладчиком демонстрируются страницы действующего Веб-портала и документы различных типов, созданные с использованием технологии КОД.

Литература

1. Липень В.Ю. Экспериментальная система «Контроль обращения документов / В.Ю.Липень [Д.В.Липень, Л.Н.Ловчева, Е.Н.Сбитнева, В.Ф.Тарасевич] // Развитие информатизации и государственной системы научно-технической информации: материалы VIII Междунар. конф. РИНТИ-2009 Беларусь, Минск, 16 ноября 2009 г. – Минск, 2009. – С. 81-85.

2. Абламейко, С.В. Защита электронных и бумажных документов в системах предоставления государственных информационных услуг / С.В. Абламейко, В.Ю. Липень // Управление информационными ресурсами: материалы V Междунар. науч.-практ. конф., Минск, 17 мая 2007 г. – Минск, 2007. – С. 267-280.

3. Липень В.Ю. Об использовании технологии «Штрих-код» для создания и верификации документов / В.Ю. Липень [и др.] // Комплексная защита информации: материалы XI Междунар. науч.-практ. конф., Новополоцк, Беларусь, 20-23 марта 2007 г. – Минск: Амалфея, 2007. – С. 153-156.

4. Липень, В.Ю. Криптографические процедуры создания и верификации идентификаторов документов и товаров / В.Ю. Липень // Технические средства защиты информации: материалы VI Бел.-росс. науч.-техн. конф., Минск, 21-22 мая 2008 г. / БГУИР. – Минск, 2008. – С. 20-21.

5. http://news.tut.by/148065.html

6. Берник, В.И. Метод создания и верификации криптографических идентификаторов и программный комплекс для его реализации / В.И. Берник, Н.И. Калоша, В.Ю. Липень // Комплексная защита информации: материалы 14-й Междунар. науч.-практ. конф., Могилев, 19-22 мая 2009 г. – Могилев, 2009. – С. 36-37.

7. Метод формирования и верификации уникальных криптографических идентификаторов / В.И.Берник [Н.И.Калоша, В.Ю.Липень, Д.В.Липень] // Технические средства защиты информации: материалы VII-ой Белорусско-рос. науч.-техн. конф., Минск, 23-24 июня 2009 г. / БГУИР – Минск, 2009. – С. 1.

8. http://www.respublika.info/4935/science/article37061/

9. http://e-vote.basnet.by/infotech

Д.А.КОСТЮК, С.С.ДЕРЕЧЕННИК

ПОСТРОЕНИЕ ПРОЗРАЧНЫХ ВИРТУАЛИЗОВАННЫХ ОКРУЖЕНИЙ ДЛЯ ИЗОЛЯЦИИ УЯЗВИМЫХ ПРОГРАММНЫХ СИСТЕМ

По статистике средний компьютер большую часть времени использует не более 5-7% своей вычислительной мощности. Современные системы виртуализации лишь незначительно увеличивают этот показатель, но взамен пользователь получает ощутимо более гибкую и удобную в управлении среду. Гостевая операционная система (ОС), запускаемая в виртуализованном окружении, абстрагирована от разнообразия компьютерных комплектующих и необходимых драйверов, менее подвержена внешним угрозам безопасности. Для нее становится доступным мгновенное восстановление от сбоев и нарушения работоспособности ПО благодаря механизму снимков (snapshots) виртуальной машины (ВМ), что позволяет не только возвращать систему к сохраненному состоянию, но и легко тиражировать готовое к использованию виртуализованное окружение [1, 2].

Понятие виртуализации рабочих станций (desktop virtualization) в настоящий момент используется в двух вариациях. В более распространенном случае ВМ с гостевой ОС запускается на сервере локальной сети, а рабочая станция играет роль удаленного терминала. Для используемых при таком подходе т.н. тонких клиентов характерны редуцированные аппаратные ресурсы и низкое энергопотребление. Во втором случае хост-система с ВМ и гостевой ОС устанавливается непосредственно на рабочую станцию, и пользователь имеет выбор, работать ли с хост-системой, или с гостевой.

Прозрачная виртуализация, в нашем понимании, предполагает только опосредованное взаимодействие пользователя с ВМ, скрывая разницу между запуском ОС на хост-системе и в гостевом окружении. Такое прозрачное взаимодействие характерно для виртуализации рабочих станций, построенной в рамках первого подхода. Однако на практике нередки ситуации, когда использование централизованного терминального сервера и тонких клиентов оказывается нецелесообразным [1]. Более характерна совместная работа в локальной сети стандартных офисных компьютеров. Хотя приемлемые готовые решения, предоставляющие для такой системы прозрачную виртуализацию, отсутствуют, она может быть сравнительно легко организована с применением ряда программных пакетов с открытым исходным кодом.

Рассмотренная задача решалась нами на примере виртуализации учебного класса университета для помещения ОС от Microsoft, программирование для которых входит в учебные программы ряда профильных специальностей, в изолированные окружения, с переносом функций аутентификации пользователей на более защищенную хост-систему. Изоляция гостевой ОС от внешней сетевой активности и делегирование задач аутентификации хост-системе позволяет решить следующие проблемы:

– упростить (либо вообще исключить необходимость) восстановления системы после некорректных действий пользователей либо активности вредоносного ПО;

– избавить рабочие станции от необходимости в антивирусном мониторе, требующем регулярных обновлений и периодически ощутимо снижающем производительность системы;

– затруднить ряд несанкционированных активностей, в первую очередь связанных с сетевым взаимодействием между рабочими станциями.

Персональные компьютеры типичного для вузов учебного класса подвергаются постоянной смене пользователей, эксплуатируются совместно с широким спектром прикладного программного обеспечения, часто страдают от неквалифицированных действий пользователей и их безответственного отношения к возможности распространения вредоносного программного кода. Таким образом, учебный класс оказывается подходящим полигоном для тестирования технологий защиты и автоматического восстановления программного обеспечения в среде со сложной и динамичной картой распределения неблагоприятных факторов [3].

Особенности типичного офисного оборудования (в первую очередь отсутствие аппаратной поддержки виртуализации в дешевых процессорах) оставляет систему виртуализации Oracle VirtualBox в качестве единственного решения приемлемой производительности, не требующего оплаты лицензий и обладающего открытым исходным кодом (нами использована полностью открытая версия системы без проприетарных модулей расширения SUN/Oracle). По аналогичной причине в качестве хост-системы выбрана ОС GNU/Linux. Если возможность бесплатного использования выбранного ПО актуальна для вузов, то доступ к исходным кодам с возможностью их аудита может оказаться важным фактором для потребителя, нуждающегося в изоляции уязвимых систем средствами заведомо безопасного (свободного от оставленных производителем брешей в защите) программного решения.

Изначально проект VirtualBox не предусматривает многопользовательской работы с отдельной ВМ. Однако перенос ее конфигурации из домашнего каталога пользователя в общедоступную область и помещение ссылки на него в шаблон домашних каталогов

обеспечивает раздельный доступ к ВМ нескольких пользователей, обладающих соответствующими правами доступа. При необходимости ограничить доступ к администрированию ВМ для запуска гостевой ОС может применяться упрощенный полноэкранный интерфейс, а доступ к основному интерфейсу ограничивается на уровне прав пользователей.

Сеть гостевой системы VirtualBox, по умолчанию, настроена в режиме трансляции адресов, и ВМ не имеет реального сетевого адреса. Результатом является недоступность гостевой ОС извне при сохранении комфортного доступа из нее к сетевым сервисам – в точности так же, как это происходит с рабочими станциями локальной сети, имеющими только локальные сетевые адреса и соединяющимися с внешней сетью proxy-сервером. Данный режим является предпочтительным, т.к. ограничивает нежелательные сетевые взаимодействия для вирусов и возможного шпионского ПО. Однако если сетевое взаимодействие необходимо (например, в учебных целях), режим может быть изменен с выделением ВМ внешних сетевых адресов – ценой незначительного роста вычислительной нагрузки и снижения защищенности гостевой ОС [1].

Для упрощения администрирования компьютерного парка и с учетом отсутствия закрепления рабочей станции за конкретным пользователем в учебном классе, в сети организован сервер аутентификации, хранящий дерево учетных записей пользователей и предоставляющий к нему доступ средствами OpenLDAP. Хост-системы рабочих станций, работающие под управлением дистрибутива GNU/Linux, получают доступ к учетным записям и персональным файлам пользователя на файл-серверах сети с помощью стандартных модулей системы аутентификации Linux. При этом рабочие станции различаются только IP-адресом, выделяемым им сервером с привязкой к MAC-адресам сетевых адаптеров, и имеют идентичный дисковый образ, не требующий модификации, что выгодно отличается от невиртуализованного решения с ОС от Microsoft, работающей под управлением контроллера домена [3]. Каталоги файл-сервера однотипно монтируются в файловую систему рабочей станции как при входе пользователя в гостевое окружение, так и при входе в графическую оболочку на хост-системе. В качестве последней используется окружение рабочего стола GNOME, поэтому входом пользователя управляет менеджер сеансов GDM. Для обеспечения прозрачности доступа к виртуализованному окружению, запуск нужной ВМ включен в список доступных графических оболочек на хост-системе и выбирается пользователем при вводе логина и пароля в менеджере сеансов GDM. Так как современные версии GDM сохраняют информацию о предпочитаемом менеджере сеанса для каждого пользователя, выбор гостевой ОС в списке производится только при первом входе или при необходимости изменить предпочтения.

Доступ гостевой ОС к автоматически монтируемым ресурсам файл-сервера осуществляется через механизм разделяемых папок (shared folders) VirtualBox, позволяющий получить доступ из гостевой системы к заданному каталогу хост-системы.

Таким образом, гостевая система работает в однопользовательском режиме, автоматически монтируя при запуске каталоги хост-системы, уже отображающие необходимые для конкретного пользователя сетевые ресурсы. Монтируемые каталоги хост-системы сами являются подмонтированными файловыми системами, поэтому их подключение в качестве «сетевых» ресурсов гостевой ОС возможно только при уже запущенной ВМ. В качестве менеджера сеанса запускается несложный скрипт, в свою очередь запускающий ВМ (в полноэкранном режиме), подключающий необходимые точки монтирования и ожидающий завершения ее работы.

Дисковый образ гостевой ОС при завершении сеанса работы автоматически откатывается к исходному состоянию (фиксация дискового образа выполняется функцией «immutable disk image» VirtualBox). Гостевое окружение благодаря этому становится «неповреждаемым», что позволяет безопасно работать в нем с правами администратора.

При необходимости автоматизировать передачу USB-накопителей в гостевое окружение, проброс может автоматически выполняться VirtualBox, для чего необходимо создание соответствующего фильтра устройств в настройках. Фильтрация USB-устройств позволяет в ряде случаев обеспечить дополнительную безопасность гостевой системы: например, может быть разрешен только проброс аппаратных ключей защиты, с игнорированием накопителей и других устройств, подсоединяемых к USB-разъемам.

Таким образом, процесс подготовки рабочей станций состоит из ряда этапов, требующих ознакомления с технической документацией, редактирования конфигурационных файлов и создания несложных скриптов. Дополнительно предполагается наличие как минимум одного сервера аутентификации, а также файл-сервера с личными каталогами пользователей и, вероятно, интегрированным антивирусом ClamAV. Однако результатом является универсальный, тиражируемый без дополнительных настроек дисковый образ, рассчитанный на запуск как минимум двух ОС и изолирующий более уязвимую (менее надежную) из двух систем. Получаемое гостевое окружение не требует от пользователя непосредственного взаимодействия с дополнительным системным ПО, и при этом приобретает достоинства, нехарактерные для ОС семейства Windows. В первую очередь, это полная устойчивость к выполнению вредоносных воздействий при сохранении полного доступа пользователей к функциям администрирования. Кроме того, в гостевом окружении ОС Windows получает, по сравнению с установкой непосредственно на хост-систему, повышенные производительность и скорость реакции. Последнее обеспечивается как эффективностью файлового кэширования GNU/Linux, так и косвенными факторами: отсутствием влияния антивирусного монитора и постоянным сохранением высокой скорости реакции, характерной для только что установленных версий Windows.

Литература

1. Д. Костюк, А. Приступчик. Особенности прозрачной виртуализации небезопасных и уязвимых систем для упрощенного администрирования учебных классов // Свободное программное обеспечение в высшей школе: тезисы докладов 6-й конференции (Переславль-Залесский, 29–30 января 2011 г.). – М.: Институт логики, 2011. – С. 66– 68.

2. П.С. Пойта, В.И. Драган, А.П. Дунец, Д.А. Костюк, В.И. Хведчук, С.С. Дереченник. Подход к модернизации гетерогенной сетевой инфраструктуры на примере информационно-вычислительной сети университета // Вестник БрГТУ. – 2010. – №5: Физика, математика, информатика. – С. 75–78.

3. Д.А. Костюк, Р.В. Сченснович. Использование в образовательном процессе вычислительных сетей на базе Windows Server 2008 // Информационные технологии в образовании: материалы Международной научно-практической конференции (Минск, 21–22 мая 2009). – Мн.: БНТУ, 2009. – С. 109–113.

А.М. КРИШТОФИК, В.В. АНИЩЕНКО

СОЗДАНИЕ И ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОГО ВЫСОКОПРОИЗВОДИТЕЛЬНОГО ПРОСТРАНСТВА (КИБЕРИНФРАСТРУКТУРЫ) СОЮЗНОГО ГОСУДАРСТВА

Необходимым условием функционирования экономики современного развитого государства, избравшего путь построения экономики, основанной на знаниях, является национальная информационная вычислительная инфраструктура (часто используют термин «киберинфраструктура»), которая базируется на наборе технологий, в котором господствующие позиции занимают высокопроизводительные вычислительные средства