Д. А. Костюк, А. М. Приступчик
Брест, Брестский государственный технический университет

Особенности прозрачной виртуализации небезопасных и уязвимых систем для упрощённого администрирования учебных классов

Аннотация

Рассмотрен подход к организации прозрачной виртуализации, применённый для изолированного запуска ОС семейства Windows на типовых компьютерах учебных классов. Приведены особенности совместного применения ряда свободных программных продуктов, позволяющие избавить пользователя от взаимодействия с интерфейсом виртуальной машины, а также делегировать функции авторизации и работы с сетью базовой ОС GNU/Linux при сохранении иллюзии сетевой работы гостевой ОС. Обеспечивается экономия средств на антивирусных лицензиях, а также более высокие стабильность и скорость работы гостевой ОС по сравнению с ее невиртуализованной установкой.

Большую часть времени средний компьютер использует менее 5–7% вычислительной мощности. Системы виртуализации незначительно увеличивают этот показатель, давая пользователю взамен удобную в управлении среду — абстрагированную от разнообразия оборудования, менее подверженную угрозам, мгновенно восстанавливающуюся после сбоев. Виртуализация особенно полезна при исследовании вредоносного кода, а также при работе с ОС, ненадёжность и/или слабая защищённость которых позволяет приравнять их к данной категории.

Виртуализация рабочих станций (PC) встречается в двух вариантах. Виртуальная машина (ВМ) может быть установлена на сервер (с доступом пользователей через энергоэффективные терминалы, обладающие редуцированными ресурсами), либо на полноценную PC, пользователь которой выбирает, работать ли с хост-системой или с гостевой ОС. Прозрачная виртуализация предполагает только опосредованное взаимодействие пользователя с ВМ, скрывая разницу между запуском ОС на хост-системе и в гостевом окружении.

Применению тонких клиентов в учебных классах часто препятствует ряд причин: наличие ранее купленных офисных PC, слабый ценовой разрыв между офисным компьютером и тонким клиентом, возможная невыгодность использования устаревшего оборудования в

качестве тонких клиентов с т.з. распределения бюджета на обновление компьютерного парка, требования к сетевому оборудованию.

Типичным остаётся построение компьютерного класса на базе стандартных офисных PC. Несмотря на отсутствие приемлемых готовых решений, прозрачная виртуализация может быть организована на таких системах с применением ряда свободных продуктов.

Нами решалась задача прозрачной виртуализации учебного класса для помещения ОС от Microsoft (программирование для которых входит в учебные программы профильных специальностей) в изолированные окружения — «песочницы» (sandbox). Полученное решение позволяет:

- автоматизировать восстановление ОС;
- избавиться от антивирусных мониторов на PC (соответственно от обновления их баз и оплаты лицензий);
- осложнить непредусмотренную учебным процессом активность, связанную с динамичной 3D-графикой и сетевым взаимодействием между PC.

Особенности типового оборудования учебных классов (дешёвые процессоры без аппаратной поддержки виртуализации) оставляют VirtualBox в качестве практически единственного приемлемого решения, с переносом его конфигурации в общедоступную область и ссылкой на неё в шаблоне домашних каталогов для раздельного многопользовательского доступа к ВМ.

Т.к. сеть ВМ по умолчанию работает в режиме NAT, гостевая ОС недоступна извне при сохранении доступа из неё к сетевым сервисам. Данный режим предпочтителен для учебного класса когда учебные задания не требуют отработки сетевых взаимодействий.

В применённом нами подходе пользователи авторизуются только на хост-системах, которые работают под управлением Linux. При этом используется сервер аутентификации на OpenLDAP, а хост-системы получают доступ к учётной записи и файлам пользователя с помощью модулей pam_ldap и pam_mount. PC имеют идентичный дисковый образ, не требующий модификации, в отличие от образов ОС от Microsoft, когда те работают под управлением контроллера домена.

Доступ к общему сетевому диску с методическими материалами и к персональным каталогам может строиться на протоколах CIFS или NFS. Сетевые ресурсы монтируются хост-системой при авторизации пользователя, а доступ гостевой ОС к ним осуществляется через ме-

ханизм Shared Folders, организующий «сетевой» доступ из ВМ к каталогам хост-системы. Эта дополнительная прослойка между файл-сервером и клиентом обеспечивает:

- согласованность с использованием NAT и ограничением взаимодействия между ВМ;
- идентичность образов гостевой ОС, работающей в однопользовательском режиме;
- абстрагирование от используемого файл-сервером протокола.

Т.о., несмотря на однопользовательский режим работы, гостевая ОС монтирует при запуске каталоги хост-системы, отображающие ресурсы для конкретного пользователя.

В ВМ настроен автоматический откат образа к исходному состоянию при завершении сеанса, благодаря чему работа в ней с правами администратора и без антивируса становится безопасной (при работе антивируса ClamAV в связке с SAMBA или модулем ядра на файл-сервере).

Прозрачная виртуализация гостевой ОС обеспечена включением на хост-системе в список сеансов GDM скрипта, запускающего ВМ с подключением к ней нужных точек монтирования. При необходимости проброс USB-накопителей в ВМ может выполняться автоматически через подсистему udev.

Результатом является тиражируемый без дополнительных настроек образ, рассчитанный на запуск как минимум двух ОС с изоляцией ненадёжной системы. Помимо полной устойчивости к вредоносным воздействиям при делегировании студентам прав администратора, гостевая ОС приобретает также повышенную производительность по сравнению с установкой Windows на PC — за счёт лучшей производительности дисковой подсистемы Linux, отсутствия антивирусного монитора и сохранения отзывчивости, характерной для свежеустановленных ОС от Microsoft.