ДОВЕРЕННАЯ СРЕДА

УДК 004

DOI: 10.52190/2073-2600_2021_1_11

Применение подходов и средств создания доверенного сеанса связи для безопасной работы гипервизоров в системах виртуализации

А. Д. Хмельков
ОКБ САПР, Москва, Россия

Рассмотрены методы защиты гипервизоров от несанкционированного внесения изменений в образ. Предложен новый метод защиты.

Ключевые слова: гипервизоры, ESXi, несанкционированный доступ, доверенная загрузка, доверенный сеанс связи.

Технологии виртуализации приобретают всё большую популярность. Это подтверждается как личными наблюдениями автора, так и результатами исследований (см. например, [1—3]). Виртуализация позволяет использовать ресурсы одной и той же физической ЭВМ различным пользователям с сохранением изоляции виртуальных машин различных пользователей и с возможностью использования удалённого доступа к ресурсам ЭВМ. Для обеспечения управления виртуальными машинами на физической ЭВМ (назовём её сервером) необходим гипервизор — программное или программно-аппаратное средство, устанавливаемое на сервер и предоставляющее доступ к его ресурсам.

Цель работы — рассмотреть методы защиты гипервизоров от несанкционированного доступа (НСД), провести обзор существующих решений, а также предложить новый метод на основе создания доверенного сеанса связи (ДСС). Актуальность темы заключается в том, что развитие технологий виртуализации ведёт к увеличению количества атак на эти системы, а существующие решения обладают рядом недостатков. Новизна работы состоит в том, что в ней предложено решение, в котором гипервизор расположен на защищённом от записи разделе внешнего носителя, что автоматически гарантирует его целостность при загрузке.

Хмельков Алексей Дмитриевич, программист.
E-mail: a.hmelkov@okbsapr.ru

Статья поступила в редакцию 11 декабря 2020 г.

Материалы и методы

Для решения поставленных задач сначала подробнее опишем объект исследования — гипервизоры, затем проведём обзор существующих решений, опишем их недостатки и далее предложим новое решение, для которого не будут характерны недостатки уже имеющиеся.

Гипервизоры бывают двух типов: устанавливаемые непосредственно на "железо" сервера и не требующие для своей работы операционной системы, а также те, которым для взаимодействия с "железом" требуется операционная система. В данной статье мы будем рассматривать гипервизоры первого типа. Защита гипервизоров второго типа сводится главным образом к доверенной загрузке ОС, посредством которой они взаимодействуют с "железом".

По статистике к наиболее популярным гипервизорам, устанавливаемым непосредственно на "железо", относятся VMWare ESXi (далее ESXi), Hyper-V и KVM [4].

Подробнее рассмотрим решение на базе гипервизора ESXi, хотя оно также может быть реализовано на базе любого другого из пере-

численных гипервизоров. Структура разделов ESXi выглядит следующим образом: EFI-раздел, два boot-bank (основной и резервный). При переходе с версии ESXi 6 на ESXi 7 неиспользуемые для загрузки остальные разделы объединены в один, хранящийся в долговременной памяти. Структура разделов в версиях 6 и 7 представлена на рис. 1. Более подробно о структуре ESXi можно прочитать в документации [5].

Объект защиты представляет собой находящийся внутри контролируемой зоны сервер, на котором должен функционировать гипервизор ESXi. На сервере расположены защищённые (например, при помощи Аккорда-В) виртуальные машины, к которым через сеть могут подключаться клиенты. Защита клиентов и защита сети выходят за рамки исследования, так как непосредственно к защите гипервизоров не относятся, поэтому в настоящей работе рассмотрены не будут. Схема объекта показана на рис. 2. Тёмным цветом выделена область, защита которой рассматривается в данной статье.

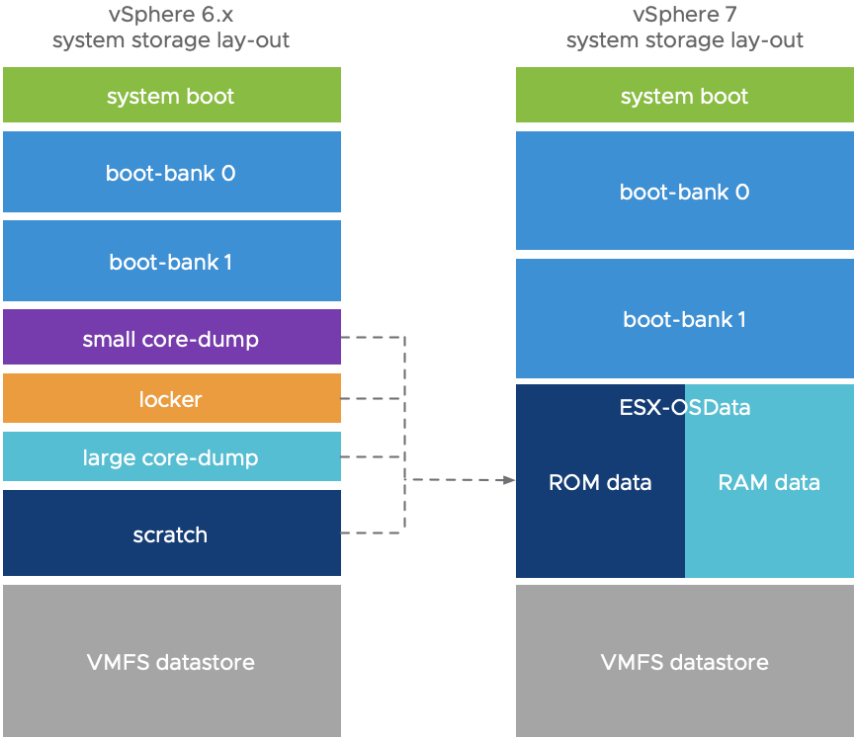

Рис. 1. Структура разделов ESXi в версиях 6 и 7

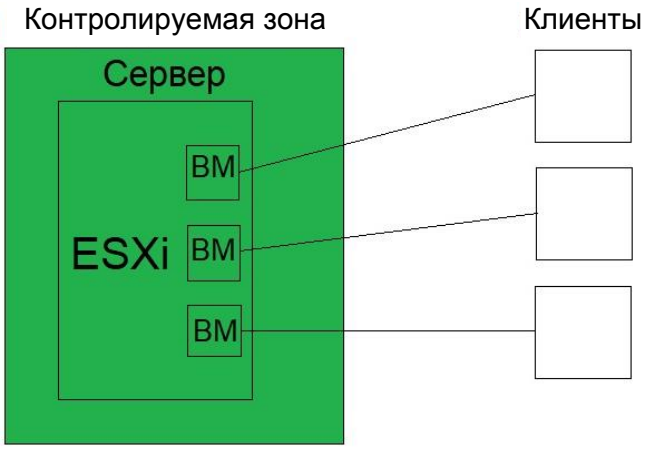

Рис. 2. Схема объекта

Для гипервизоров характерно наличие угрозы НСД, точнее одной из разновидностей НСД — несанкционированного внесения изменений в образ гипервизора, в результате которого может быть нарушена целостность программного обеспечения (например, установлено вредоносное ПО). Нарушение работы гипервизора может привести к нарушениям работы сервера, что, в свою очередь, может повлечь нежелательные последствия и на клиентских ЭВМ (например, возможны отказ в обслуживании или распространение вредоносного ПО).

Обзор литературы

Существует несколько подходов по обеспечению защиты гипервизора от НСД. Один из них — использование средств доверенной загрузки (СДЗ), таких, как Аккорд-АМДЗ, о котором подробнее можно прочитать в [6], Инаф, Средства доверенной загрузки (СДЗ) уровня BIOS. Данный метод надёжен, но имеет ряд недостатков. Для использования Аккорда-АМДЗ необходимо наличие свободного слота PCI-express, который имеется не на всех современных серверах. Для подключения Инаф необходим свободный USB-порт, которых может быть мало. Кроме того, USB-порт необходим для подключения аппаратного идентификатора, работающего с СДЗ. СДЗ уровня BIOS не требует ни слота PCI-express, ни USB-порта (кроме как для идентификатора), но в некоторых серверах BIOS защищён от записи программными средствами, а использование программатора может быть затруднено, если чип с BIOS не является съёмным.

Альтернативный подход к обеспечению защиты гипервизора от НСД — использование средства обеспечения доверенного сеанса связи (подробнее о концепции которого см. в [7, 8]). Это устройство представляет собой загрузочную флэшку с несколькими разделами, для каждого из которых установлены свои политики чтения и записи, способные меняться при вводе корректного пин-кода [9]. ESXi можно разместить на разделе с правами Read only, с которого и будет производиться загрузка. В результате будет решена проблема целостности объектов гипервизора, т. е. не надо будет дополнительно проверять целостность компонентов гипервизора, а сам носитель, если его выставить первым загрузочным устройством в настройках BIOS сервера, будет выполнять функции перехвата управления. Таким образом, получится своего рода "неатомарный" РКБ, описанный в [10]. Проблема размещения ESXi на неизменяемом разделе — невозможность обновления, которое периодически требуется для гипервизора. Решением данной проблемы может стать временный перевод раздела с ESXi в режим Read-Write (RW).

Результаты

Рассмотренные решения обладают рядом недостатков. Далее опишем устройство, для которого эти недостатки не будут характерны. Устройство представляет собой защищённый загрузочный носитель. На носителе с установленным специальным ПО, позволяющим разграничить доступ к разделам носителя, создают раздел, на который кладут ESXi. В результате получается своего рода дистрибутив ESXi на специальном носителе. Аналогичный подход применяют также, например, при создании СДЗ, которое может обеспечить доверенную загрузку нескольких серверов [11]. Раздел с ESXi по умолчанию установлен в режим RO. При запуске сервера сначала стартует специальное ПО носителя, которое затем передаёт управление ESXi, если загрузка не была прервана.

Обновления ESXi можно провести в двух режимах: автоматическом и ручном (подробнее об этом можно прочитать в документации ESXi [12]). При автоматическом обновлении ESXi будет запущен и установит предварительно помещённые на другой раздел носителя обновления своими штатными средствами. Недостаток этого метода состоит в том, что ESXi будет загружен с раздела, который можно изменять. При ручном методе данные для обновления можно записать на раздел с ESXi, не запуская сам гипервизор. Для этого необходимо посредством ПО на загрузочном разделе носителя загрузить не сам ESXi, а предварительно подготовленный раздел с обновле-

ниями. В любом случае при необходимости обновления перед стартом ESXi при помощи ПО носителя раздел временно переводят в режим RW (для перевода необходимо ввести пин-код). После установки обновлений сервер перезагружают, а раздел с ESXi вновь устанавливают в режим RO. Далее можно вновь загрузить ESXi уже с неизменяемого раздела и продолжить работу сервера в штатном режиме.

При наличии нужного числа USB-портов для подключения ещё и аппаратного идентификатора носитель со специальным ПО и ESXi можно дополнить СДЗ, выделив на носители разделы под ОС СДЗ и базу данных. При таком решении перед стартом ESXi будет сначала запускаться СДЗ для обеспечения доверенной загрузки гипервизора. Преимущество перед решением, использующим только СДЗ (например, Инаф), заключено в наличии неизменяемого раздела, с которого запускается ESXi. СДЗ может обеспечить только доверенную загрузку, а состояние сервера в процессе его работы СДЗ не контролирует. При данном решении загрузка с изменяемого раздела производится только для установки обновлений в автоматическом режиме. Схема такого носителя приведена на рис. 3.

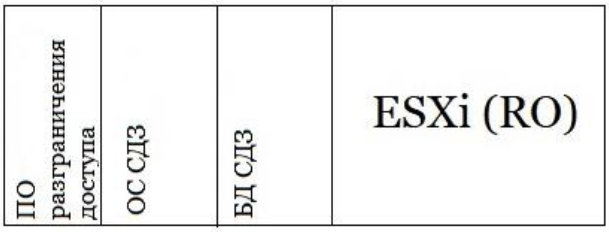

Рис. 3. Схема носителя с ПО разграничения доступа, СДЗ и ESXi

Разделы со специальным ПО и ESXi на носителе должны присутствовать обязательно, раздел с СДЗ — опционально. Если планируется проводить ручную установку обновлений, то также необходимо создать раздел, на который будут помещаться обновления.

Сценарий работы устройства таков:

- запуск специального ПО, расположенного на первом разделе носителя;
- в случае, если в течение определённого времени загрузка не была прервана, загрузка ESXi со своего раздела;
- прерывание загрузки после старта специального ПО может позволить:
  - перевести раздел с ESXi из режима RO в режим RW и обратно,
  - продолжить загрузку не с ESXi-раздела, а с раздела с обновлениями;
- при наличии СДЗ специальное ПО передаёт управление не загрузчику ESXi, а СДЗ, которое после успешного прохождения процедур идентификации-аутентификации и контроля целостности уже передаёт управление загрузчику ESXi.

Обсуждение

Данное решение применимо при условии, что сервер находится внутри контролируемой зоны, а загрузка с иных носителей или без установленного защищённого загрузочного носителя невозможна. Иначе у потенциального нарушителя будет возможность извлечь загрузочный носитель и вставить в сервер свой. Решение, не включающее СДЗ, требует одного свободного USB-слота, включающее — двух, но при этом не требует наличия PCI-слотов и возможности прошивать BIOS сервера. Расположение гипервизора на неизменяемом в основном режиме работы разделе гарантирует целостность гипервизора, а возможность перевода раздела с гипервизором в режим RW даёт возможность обновления. Безопасность обновления обеспечивает либо загрузка с раздела с обновлениями, либо проверка целостности раздела с гипервизором. При подобной схеме работы у злоумышленника нет возможности внедрить вредоносное ПО ни во время работы гипервизора, ни во время его обновления.

Заключение

Предложено решение, обеспечивающее защиту гипервизора от несанкционированного доступа на основе создания ДСС. Это решение позволит обеспечить целостность раздела с ESXi, возможность безопасного обновления гипервизора в ручном режиме и будет требовать наличия всего одного свободного USB-порта. Решение, включающее в себя СДЗ, по-

требует дополнительный USB-порт для подключения аппаратного идентификатора, но компенсирует этот недостаток возможностью провести доверенную загрузку ESXi с изменяемого раздела для автоматического обновления. При выполнении организационных и технических требований, возникающих из-за ограничений применимости, данное решение будет актуальным для компаний, использующих сервера с расположенными на них виртуальными машинами, безопасность подключения к которым необходимо обеспечить.

Литература

1. *Мозолина Н. В.* Защита виртуализации "в эпоху бурного развития" // Информационная безопасность. 2019. № 1. С. 29.
2. *Каннер А. М.* Разграничение доступа в Linux при использовании средства виртуализации kvm // Вопросы защиты информации. 2019. № 3. С. 3—7.
3. *Маляревский А.* Виртуализация как тренд 2020 [Электронный ресурс]. URL: https://www.crn.ru/news/detail.php?ID=141879
4. Сравнение гипервизоров: KVM, Hyper-V или VMware? [Электронный ресурс]. URL: https://www.xelent.ru/blog/sravnenie-gipervizorov-kvm-hyper-v-ili-vmware/
5. Что изменилось в структуре дисковых разделов (Partition Layout) на платформе WMware vSphere 7? [Электронный ресурс]. URL: https://www.vmgu.ru/news/vmware-vsphere-7-disk-partition-layout
6. *Конявский В. А.* Управление защитой информации на базе СЗИ НСД "Аккорд". — М.: Радио и связь, 1999. — 325 с.
7. *Каннер А. М.* Средство организации доверенного сеанса как альтернатива доверенной вычислительной среде // Информационные технологии управления в социально-экономических системах. 2010. Вып. 4. С. 140—143.
8. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ!: мат. XV Междунар. науч.-практ. конф. "Комплексная защита информации". (Иркутск), 1—4 июня 2010 г.
9. *Чугринов А. В.* Доверенные сеансы связи и средства их обеспечения // Информационная безопасность. 2010. № 4. С. 54—55.
10. *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности: материалы XX науч.-практ. конф. "Комплексная защита информации", Минск, 19—21 мая 2015. С. 53—55.
11. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды // Вопросы защиты информации. 2014. № 4. С. 64—68.
12. VMware ESXi Upgrade [Электронный ресурс]. URL: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.esxi.upgrade.doc/

Trusted communication session approaches and tools application for the safe operation of hypervisors in virtualization systems

A. D. Khmelkov
OKB SAPR, Moscow, Russia

Methods of protecting hypervisors from unauthorized changes to their images are considered. A new method of protection is proposed.

Keywords: hypervisors, ESXi, unauthorized access, trusted boot, trusted communication session.

Bibliography — 12 references. *Received December 11, 2020*