ЮГО-ЗАПАДНОЕ ОКРУЖНОЕ УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
ДЕПАРТАМЕНТА ОБРАЗОВАНИЯ
ГОРОДА МОСКВЫ

ГБОУ ШКОЛА №1533 ”ЛИТ”

ТЕЗИСЫ РАБОТЫ

(специальность ”Прикладное программрование”)

учащегося группы 11.3
Захарова Ильи Александровича

Разработка гипервизора Jinet

Научный руководитель: Байков Б. К.,
ведущий системный разработчик,
«Т-Платформы»

Консультанты: Потёмкин А.В
Гиглавый А.В.
Завриев Н.К.
Труфанов Д.С.

Москва — 2017

Содержание

1 Введение

Гипервизор – это программа, обеспечивающая разделение ресурсов компьютера на несколько виртуальных машин, и запуск на каждой виртуальной машине своей операционной системы.

Такая программа обеспечивает либо разделяемый, либо монопольный доступ виртуальных машин к каждому из аппаратных устройств компьютера. Создаются виртуальные устройства, конфигурация которых может отличаться от конфигурации устройств аппаратных.

Виртуализация позволяет эффективно и безопасно разделять работающие приложения друг от друга. Виртуальные машины не могут влиять на ход работы друг друга, и, если скомпрометирована одна виртуальная машина, все остальные остаются в безопасности. Поэтому она используется в самых разных областях IT. Зачастую виртуализацию также используют для эффективного сегментирования ресурсов компьютера на отдельные виртуальные машины.

Была поставлена задача написать минимальный учебный демонстрационный гипервизор. Исходный текст проекта выпущен под лицензией MIT.

2 Актуальность

С каждым годом технологии виртуализации всё глубже и глубже входят в мир информационных технологий, находя применения в самых разных областях IT:

1. изоляция серверных систем для обеспечения их безопасности
2. эффективное сегментирование ресурсов компьютера
3. одновременное использование разных ОС на настольном компьютере
4. отладка гостевых систем через вывод всех выходов из ВМ

Для создания систем виртуализации требуются специалисты, способные понимать принципы и механизмы программной и аппаратной виртуализации. Для меня, как автора диплома, целью написания диплома стало погружение в мир виртуализации, вычислений и прямого программирования железа. Удалось узнать, как работает виртуализация изнутри и научиться писать код управления механизмами обслуживания виртуализации.

3 Постановка задачи

Идея проекта была предложена руководителем с целью изучения архитектуры x86, включая механизмы изоляции приложений и виртуальных машин друг от друга путём создания монитора виртуальных машин, он же гипервизор. Для меня это стало уникальной возможностью углубить знания архитектуры процессоров Intel и навыки системного программирования.

Цель работы – это создание минимального монитора виртуальных машин (гипервизора) с использованием механизмов аппаратной виртуализации архитектуры x86-64 (AMD64).

Были поставлены следующие задачи:

1. Обеспечить загрузку из бутсектора (bootsector)
2. Настроить режим работы видеоадаптера для отображения вывода текстовых данных
3. Настроить память в 32-битной плоской модели и осуществить переход в 32-битный защищённый режим (`Protected Mode`)
4. Настроить механизмы страничной трансляции памяти и переход в 64-битный режим (`Long Mode`)
5. Настроить обработку исключений и прерываний
6. Настроить расширения аппаратной виртуализации Intel VT-i и включение режима VMX
7. Обеспечить функционирования вызовов (VMCall) из виртуальных машин в гипервизор (монитор виртуальных машин) и возвратов обратно в виртуальные машины

4 Анализ предметной области

4.1 Виртуализация

Виртуализация – техника предоставления исполняемой программе набора вычислительных ресурсов, абстрагированная от их аппаратной реализации. Виртуализация была предметом изучения информатики на протяжении многих лет: так, например, советские инженеры решали проблему портирования программного обеспечения с платформ имеющих другие интерфейсы, нежели физический компьютер, на котором программа исполнялась.

В рамках этой работы мы будем говорить не столько о виртуализации ресурсов, сколько о работе гипервизора – программы, занимающейся разделением работы ресурсов одной фи-

зической машины (хозяин (*англ.* host)) на множество виртуальных машин (гость (англ. guest)). Внутри каждой виртуальной машины исполняется своя ОС, ход работы которой не влияет на работу других ВМ.

Гипервизор, в отличие от эмулятора, выполняющего программную эмуляциию команд, лишь перехватывает управление у виртуальных машин в случае необходимости. Код виртуальных машины выполняется аппаратно в процессоре. Так как принцип работы гипервизора предполагает изоляцию виртуальных машин, для более эффективной его работы необходима аппаратная поддержка виртуализации. Первой в этой области была компания IBM с мэйнфреймами System/360, System/370, созданными на рубеже 60-70-х годов прошлого века. Современные процессоры Intel также подерживают расширения аппаратной виртуализации (VT-i, VT-d), что значительно ускоряет процесс виртуализации.

После появления первых гипервизоров появилась необходимость создания формальных критериев виртуализации. В 1974 статья Джеральда Попека и Роберта Гольдберга их сформировала.

4.1.1 Классический критерий виртуализуемости

Требования к монитору виртуальных машин (то же, что и гипервизор) состоят из трёх пунктов:

1. **Изоляция**. Каждая ВМ имеет доступ только к своим ресурсам. Виртуальные машины не влияют на работу друг друга, если одна виртуальная машина оказалась зараженной вирусом, другая продолжает работу.

2. **Эквивалентность**. Виртуальная машина ведёт себя так же, как и настоящий компьютер с аналогичными характеристиками. Единственное различие заключается в скорости исполнения, виртуальная машина работает медленнее компьютера.

3. **Эффективность**. Статистически преобладающее подмножество инструкций виртуального процессора должно исполняться напрямую хозяйским процессором, без вмешательства монитора ВМ. Управление передаётся гипервизору только в случае привилегированной операции – той, которая может нарушить изоляцию машин.

4.1.2 Типы гипервизоров

Гипервизоры делят по их устройству на две большие группы: гипервизоры I и II типа.

- **Гипервизоры I типа** исполняются непосредственно на компьютере и имеют полный доступ к его устройствам. Компьютер загружается в софт гипервизора, и монитор ВМ, по-

добно операционной системе, начинает работы с устройствами. Примеры: VMWare ESXi, Xen. (см. рис. 1)

- **Гипервизоры II типа** загружаются внутри ОС и получают доступ к устройствам через её интерфейсы. Зачастую при установке гипервизор II типа устанавливает в ядро ОС свой модуль, с помощью которого он может обращаться к низкоуровневым процессорным расширениям виртуализации. Примеры: KVM, VirtualBox. (см. рис. 2) Гипервизор Jinet -

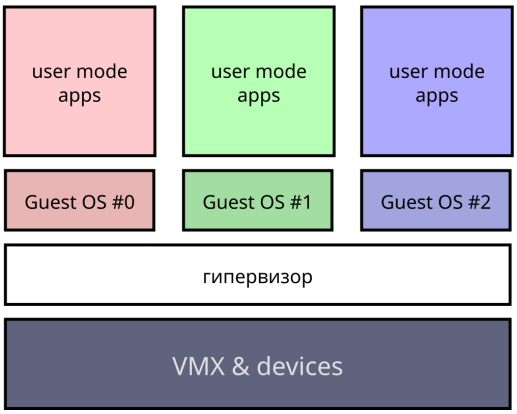

Рис. 1: I тип гипервизоров

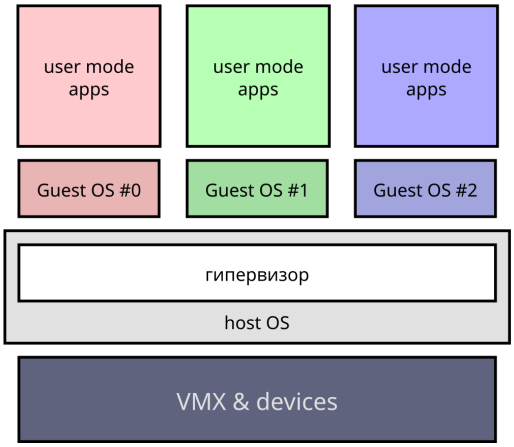

Рис. 2: II тип гипервизоров

гипервизор I типа: так легче обращаться к ресурсам компьютера.

5 Обзор аналогов

В данной работе представляется маленький гипервизор. Подобные ему большие аналоги писали десятки программистов много месяцев. Гипервизор Jinet сейчас позволяет запускать простейший код в изолируемом окружении BM виртуальной машины. У всех из предложенных ниже гипервизоров исходный текст находится в открытом доступе. Приведённые аналоги были написаны специалистами в области информационной безопасности и системного программирования. Некоторые из предложенных гипервизоров первого типа, а некоторые – второго.

[1]см. 4.1.2

Таблица 1: Аналоги

Гипервизор	Тип VMM[1]	Платформы (если II тип)	Размер исходного текста	Назначение
SimpleVisor	II	Win8.1; частично UEFI	162 KB	использование новейшего VMX
Ramooflax	I	–	2.26 MB	анализ/отладка /контроль ВМ
HyperPlatform	II	Win7; Win8.1; Win10: x86 & x64	7.64 MB	анализ работы Windows
Jinet	I	–	421 KB	учебный гипервизор

6 Программная реализация

Гипервизор Jinet был написан на языках программирования ассемблер (диалекты `fasm` и `as`) и C (компилятор `gcc`). Сборка проекта осуществляется с помощью сборщика `gnu ld` и утилиты `gnu make`. В качестве системы контроля версий используется `git` и хостинг GitHub.

7 Пример использования

На рис. 3 изображена работа гипервизор Jinet. На данный момент гиперивизор поддерживает работу виртуальной машины, которая выводит сообщение о своём успешном запуске с помощью vmcall: `Hello! I am VM1!`.

8 Результат

Была изучена архитектура процессоров Intel x86. За время работы над гипервизором пришлось изучить самые разные аспекты работы современных ПК: от работы в 16-битном режим до опыта неуспешной отладки на разработческих платах.

Рис. 3: Работа программы (VESA-режим)

Был получен важный опыт работы с технической документацией. Большая часть документации, изученной во время работы над дипломным проектом, была написана на техническом английском. При работе с такой низкоуровневой технологией, как аппаратная виртуализация, была важно консультироваться со справочниками и документацией Intel.

Был изучен инструментарий современного системного программиста. Основы статического компонования, формат исполняемых файлов `elf`, особенности встроенного ассемблера gcc – самые разные технологии системного программирования были изучены при написании данной работы. Изучались также утилиты для сборки: были написаны скрипты для сборки проекта утилитами `gnu make` и `gnu ld`, а также Python-скрипт для конфигурирования проекта.

Были изучены основы работы с языком ассемблер и работы с большими проектами на C. Были изучены три диалекта языка ассемблер: `masm`, `fasm` и `gnu as`. В работу вошёл код, написанный на последних двух. Также были изучены принципы написания интерфейсов и безопасного программирования на C.

9 Выводы

Создан гипервизор Jinet. Доказано, что можно написать гипервизор силами одного человека в короткие сроки. Многое ещё требует реализации и улучшения:

1. Доработка SeaBIOS для поддержки запуска 16-битных операционных систем
2. Поддержка ряда устройств для запуска одного из вариантов DOS
3. Поддержка гипервизором работы на нескольких ядрах, процессорах
4. Поддержка NUMA-систем

5. Поддержка технологии Intel GVT-g (представлена в 2015), делающей возможной аппаратную виртуализацию видеоадаптеров для ВМ

10 Список литературы

[1] Popek G. J., Goldberg R. P. Formal requirements for virtualizable third generation architectures // Communications of ACM. 1974.

[2] @Atakua. Аппаратная виртуализация. Теория, реальность и поддержка в архитектурах процессоров. `https://habrahabr.ru/company/intel/blog/196444/`. 2013.

[3] М. Чурдакис. The Infamous Trilogy: CPU internals, Virtualization, Raw multicore programming. `https://www.codeproject.com/articles/45788/the-real-protected-long-mode-assembly-tutorial-for`. 2015.

[4] OSDev Wiki. `http://wiki.osdev.org/Main_Page`.

[5] Intel. Intel® 64 and IA-32 Architectures Software Developer Manual. 2017.

[6] AMD. AMD64 Architecture Programmer's Manual, Volume 2: System Programming. 2017.

[7] В. Садовников. Начала программирования в защищённом режиме. `http://e-zine.excode.ru/online/1/Introduction.html`. 2006.

[8] GNU Project and Free Software Foundation. GNU Make Manual.

[9] GNU Project and Free Software Foundation. GCC Manual.

[10] GNU Project and Free Software Foundation. GNU Linker Manual.

[11] Grysztar Tomasz. flat assembler 1.71.

[12] Toshiba HP Intel Microsoft Phoenix. Advanced Configuration and Power Interface Specification, Revision 5.0a.

[13] Portable Formats Specification Version 1.1. Executable and Linkable Format (ELF).