ФРТК

iSCALARE

intel

Лаборатория суперкомпьютерных технологий для биомедицины, фармакологии и малоразмерных структур

Улучшенные техники моделирования центрального процессора

Григорий Речистов

grigory.rechistov@phystech.edu

11.03.2013

На прошлой лекции

- Интерпретатор — медленно
- Двоичный транслятор — быстрее

Прямое исполнение

- Guest ISA == Host ISA
- (Почти) все инструкции совпадают
- *Наверное*, можно исполнять их напрямую

Алгоритм

```
execute() {
   save_host_ctxt();
   set_guest_ctxt();
   setjmp(back);
   goto guest_start_ip;
   back: restore_host_ctxt();
}
```

Что же различается

- Периферийные устройства
  - Их количество, виды и размещение
- Число процессоров
- Режим процессора

Проблемы с наивным DEX

- Окружение гостя не совпадает с окружением хозяина
  - Unix libc/WinAPI (application mode) [wine is not an emulator!]
  - Периферийные устройства (full platform)
- Защита памяти хозяина
  - Гость может писать/читать любой адрес, при этом он не должен видеть/изменять данные симулятора
- Привилегированные инструкции
  - Семантика инструкции может зависеть от режима процессора. Симулятор – приложение уровня пользователя, не может исполнять все инструкции.

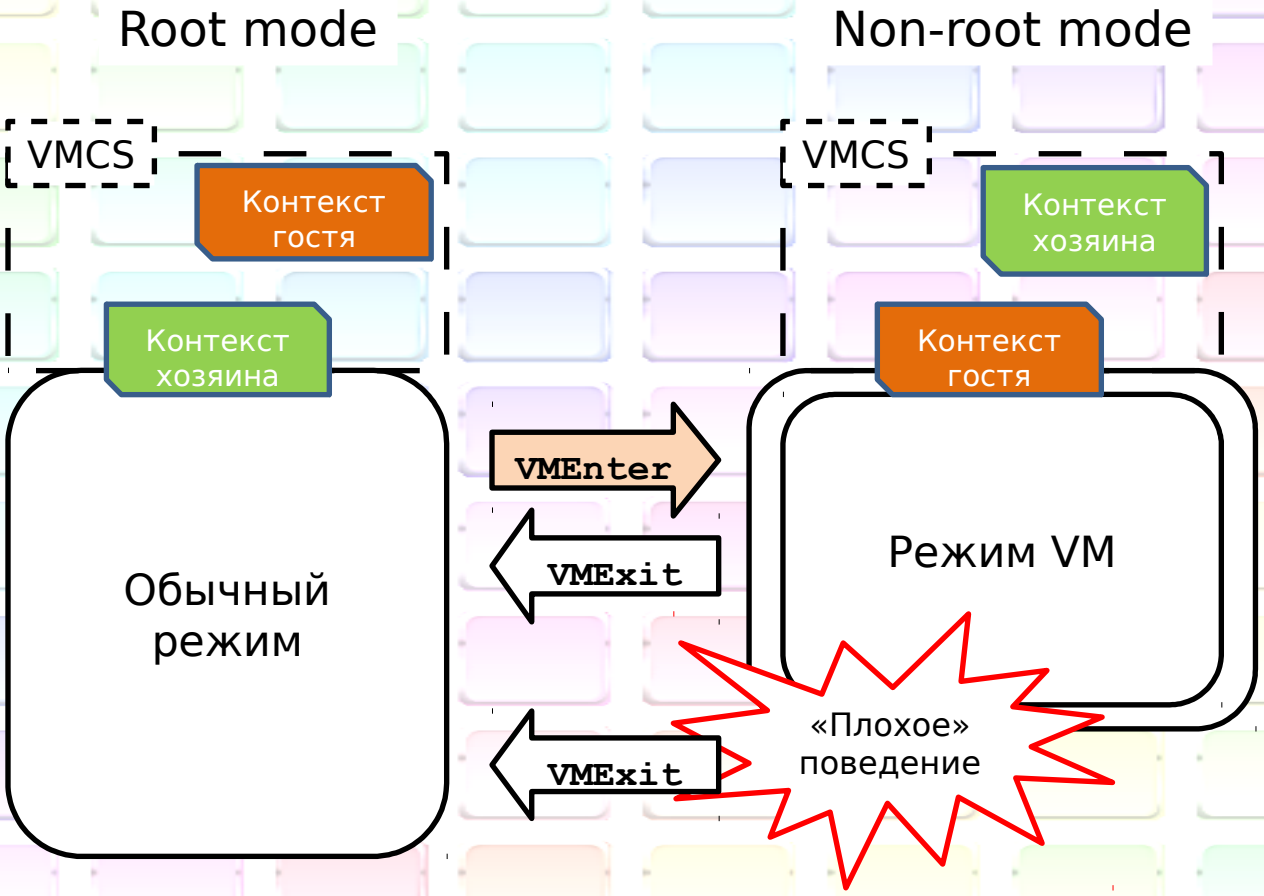
Возможное решение

- Предварительный просмотр гостевого кода на предмет опасных инструкций
- Замена таких инструкций на безопасные (вызов собственного обработчика)
- Переписывание всех доступов в память
- Пример: **`http://pintool.org/`** для IA-32, IPF, XScale

Наилучшее решение

- Аппаратная поддержка режима прямого исполнения
  - Аппаратура создаёт режим «песочницы», в котором гость может выполнять любые инструкции
  - Опасные инструкции вызывают остановку прямой симуляции и контролируемый выход в симулятор

IA-32 virtualization technology (VTx)



Principal Causes of VMEXIT

- Paging state exits allow page-table control
  - CR3 accesses, INVLPG cause exits
  - Selectively exit on page faults
  - CR0/CR4 controls allow exiting on changes to selected bits
- State-based exits allow function virtualization
  - CPUID, RDMSR, WRMSR, RDPMC, RDTSC, MOV DRx
- Selective exception and I/O exiting reduce unnecessary exits
  - 32-entry exception bitmap, I/O-port access bitmap
- Controls provided for asynchronous events
  - Host interrupt control allows delivery to VMM even when guest blocking interrupts
- Detection of guest inactivity to support VM scheduling
  - HLT, MWAIT, PAUSEs

Симулятор, использующий аппаратную виртуализацию

+ Прямое исполнение большинства инструкций
+ Упрощение модели, уменьшение объёма кода симулятора
- Необходима аппаратная поддержка
- Модуль/драйвер ядра для управления в root режиме
- Медленное переключение между root/non-root режимами
- Не все режимы процессора могут быть в non-root mode (например, real mode)
- Рекурсивная виртуализация?

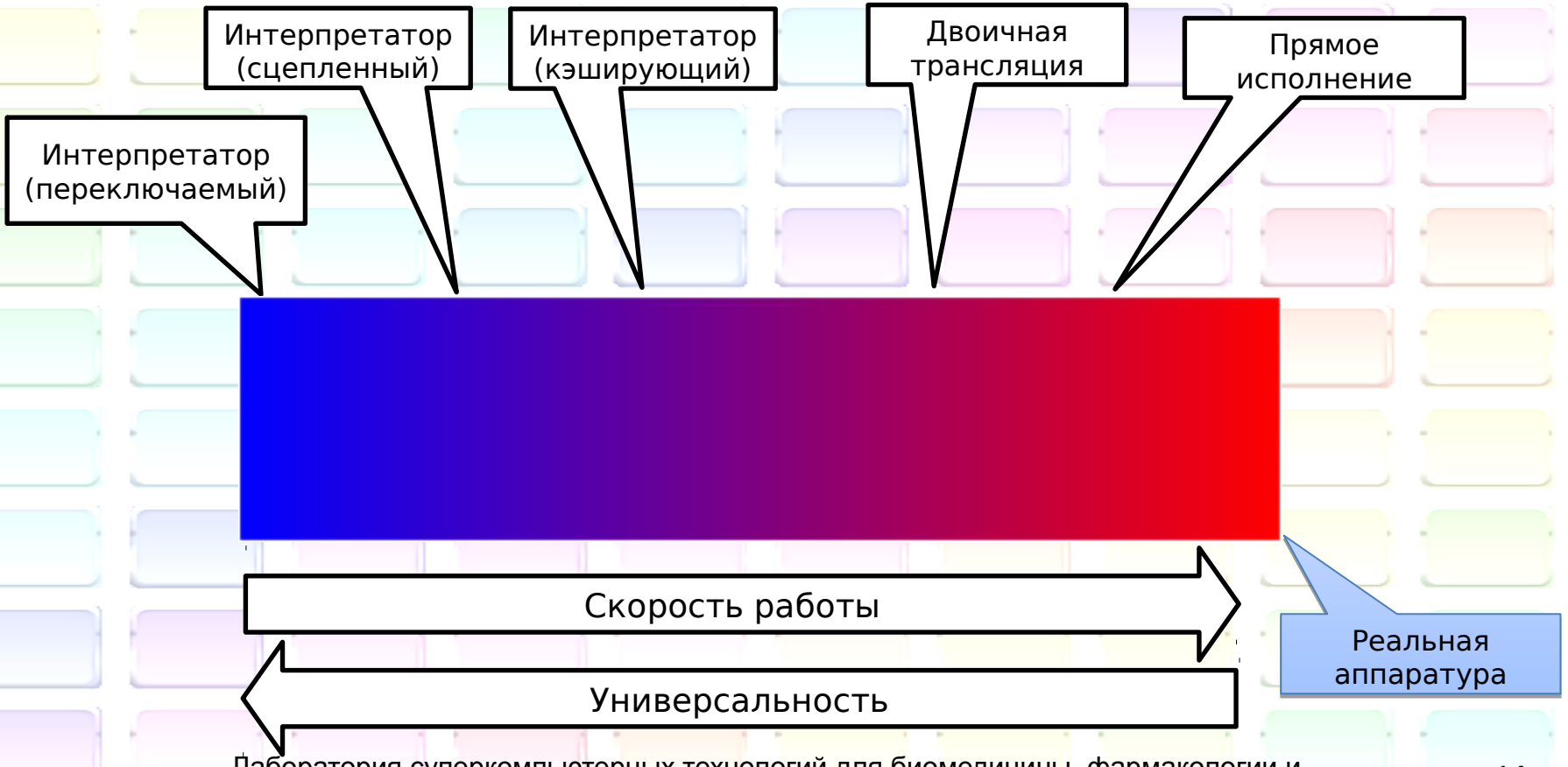
Практическое использование VTx

- VirtualBox — VTx необходим для симуляции 64 битных гостей
- Microsoft VirtualPC — VTx необходим
- Wind River Simics — VTx опционален
- VMware ESXi — VTx необходим для симуляции 64 битных гостей

Что мы имеем в результате

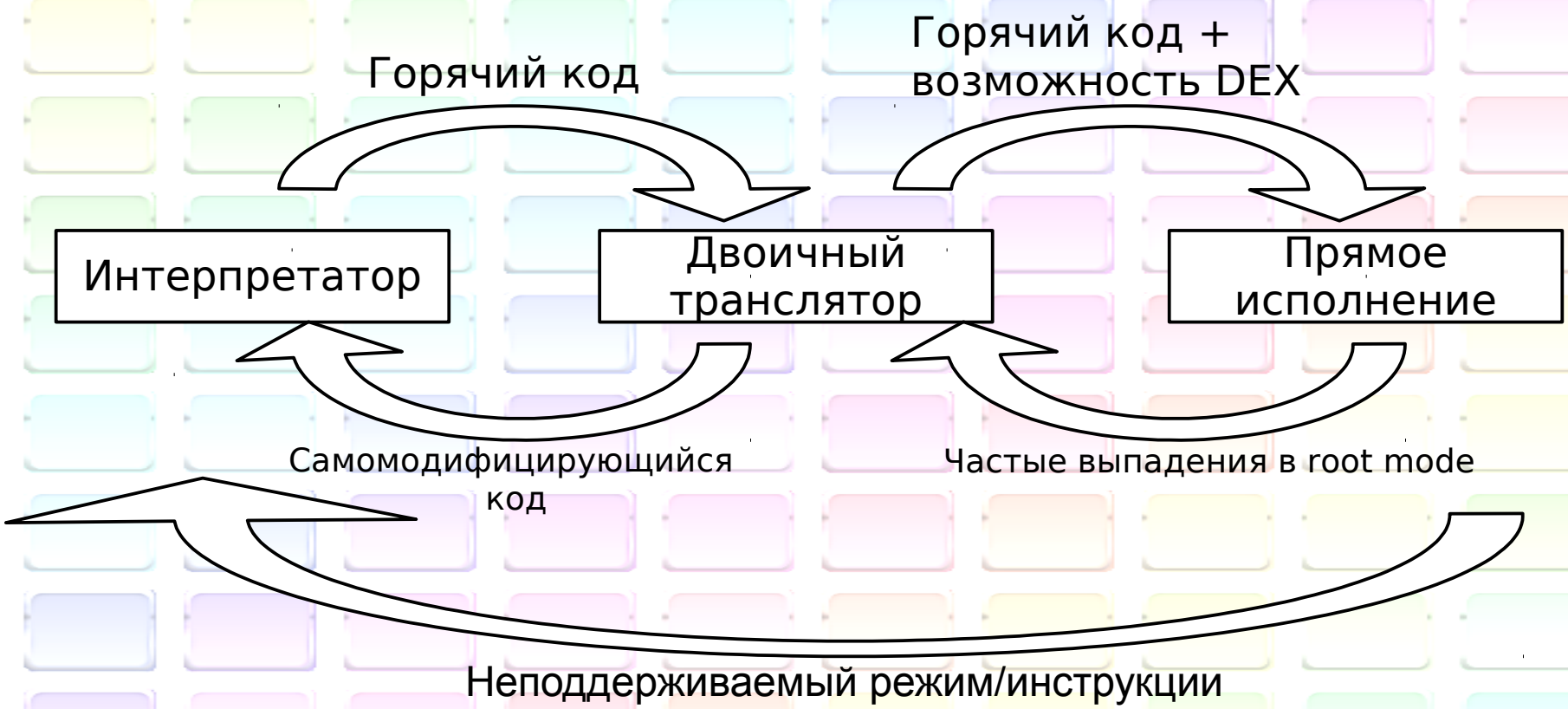
- Три техники симуляции
  - Интерпретация
  - Двоичная трансляция
  - Аппаратная поддержка
- Существуют различные сценарии симуляции, в которых каждый из подходов предпочтительнее остальных

Спектр симуляционных подходов



Решение – «коробка передач»

Динамическое переключение между режимами



Динамическое переключение между режимами симуляции

- Оптимальное использование лучших сторон каждого из подходов
- Необходимость разработки фактически трёх симуляторов

Итоги

- Наивное прямое исполнение
- DEX с аппаратной поддержкой
  - root mode, non-root mode
  - VM enter, VM exit
- Переключение режимов симуляции
  - Условия на переходы

Рекомендуемая литература

- F. Leung, G. Neiger, D. Rodgers, A. Santoni, R. Uhlig. **Intel® Virtualization Technology** // Intel Technology Journal №10 (03 Aug 2006).

http://www.intel.com/technology/itj/2006/v10i3/

- Matias Zabaljauregui. **Hardware Assisted Virtualization Intel Virtualization Technology**. 2008. **http://lib.mipt.ru/book/283035/**

На следующей лекции:

- Не центральным процессором единым
  - Полноплатформенная симуляция
  - Исполняющие и неисполняющие устройства
- Моделирование многопроцессорных систем
  - Квант (квота) времени
  - Гиперсимуляция

Спасибо за внимание!

Все материалы курса выкладываются на сайте лаборатории:
http://iscalare.mipt.ru/material/course_materials/