iSCALARE

Лаборатория суперкомпьютерных технологий для биомедицины, фармакологии и малоразмерных структур

Прямое исполнение

Григорий Речистов
grigory.rechistov@phystech.edu

24.03.2014

На прошлых лекциях

- Интерпретатор — медленно
- Двоичный транслятор — быстрее

Вопросы

- Что такое капсула в ДТ?
- Что такое блок трансляции в ДТ?
- Чем динамическая трансляция отличается от статической?
- В чём заключается проблема code discovery?

Прямое исполнение

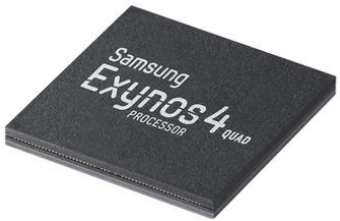
- Guest ISA = Host ISA
- (Почти) все инструкции совпадают

Гость

Хозяин

IA-32:

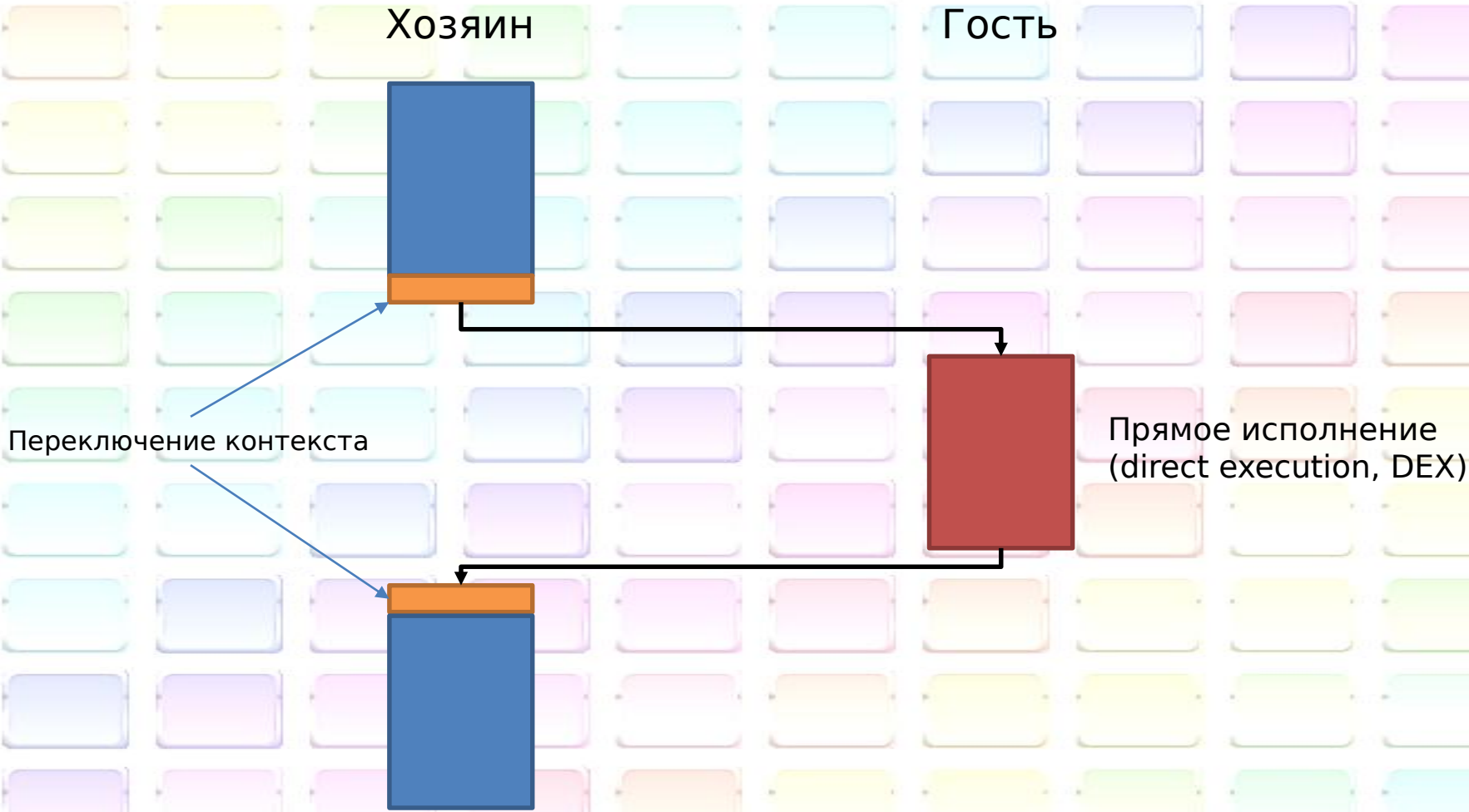
ARM:



Алгоритм (1/2)

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

Алгоритм (2/2)


Хозяин
Гость
Переключение контекста
Прямое исполнение
(direct execution, DEX)

Почему это не будет работать (1/2)

- Не полностью совпадающие ISA
- Различное положение внешних ресурсов (устройств и памяти)
- Привилегированность инструкций
- Необходимость изоляции симулятора от обнаружения/разрушения гостем

Почему это не будет работать (2/2)

```
add %r1, %r2
mul $10, %r3
div %r4, %r5
ld (0xa000), %r10
st %r10, (%r11)
sub %r11, %r1
mov $16, %r13
mov %r13, %cr0
trap $32
```

Отсутствующая в хозяине инструкция

Обращения к памяти

Привилегированные инструкции

Предпросмотр кода

- Инспектирование гостевого кода на предмет «опасных» инструкций
- Замена инструкций на контролируемые — инструментация
- «Почти» ДТ

Заплатки и заглушки

Исходный код

```
add %r1, %r2
mul $10, %r3
div %r4, %r5
ld (0xa000), %r10
st %r10, (%r11)
sub %r11, %r1
mov $16, %r13
mov %r13, %cr0
trap $32
```

Код после предпросмотра и инструментации

```
add %r1, %r2
mul $10, %r3
trap $255
ld (0xb000), %r10
st %r10, (%r11)
sub %r11, %r1
mov $16, %r13
trap $255
trap $255
```

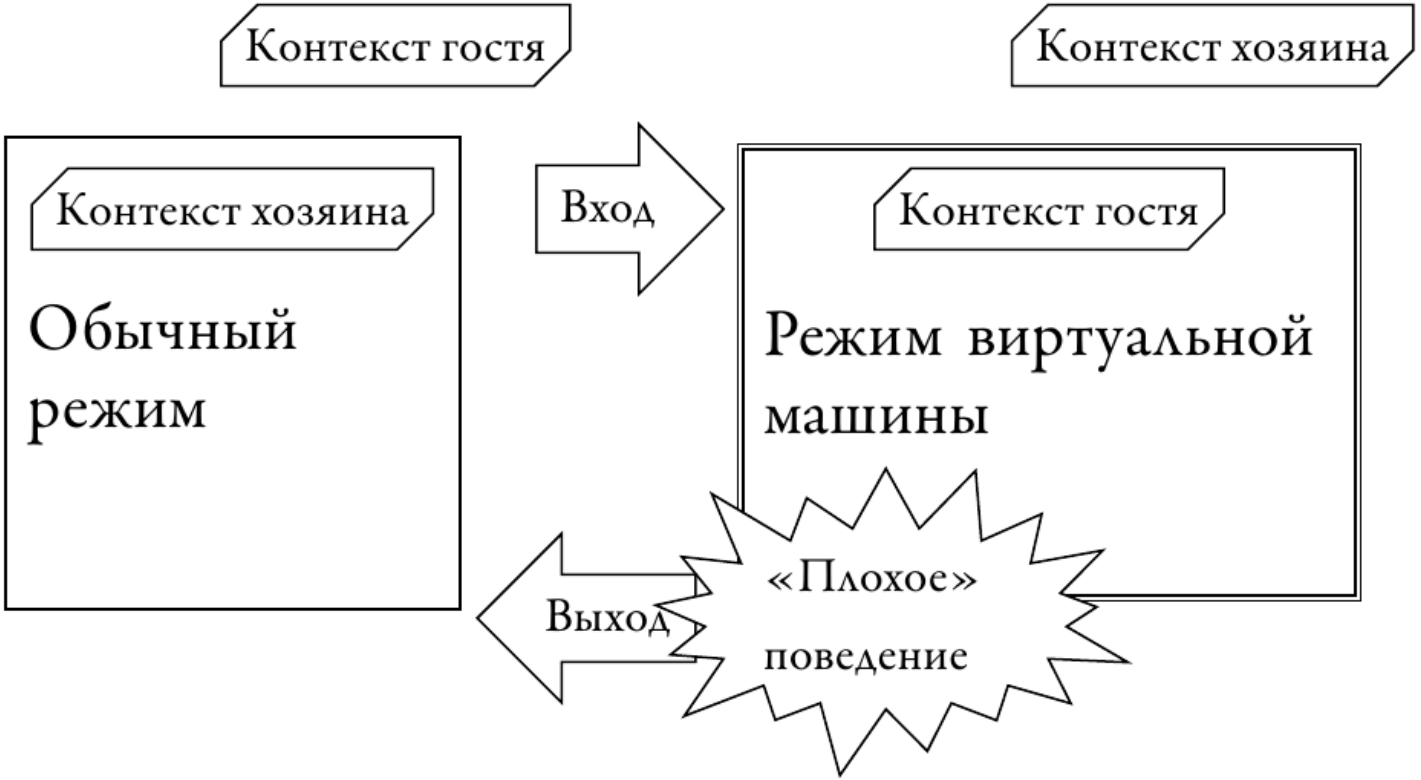
Двоичная инструментация

- Общее название методики исследования и модификации приложений
- Pin http://pintool.org
- DynamoRIO http://dynamorio.org/

Сложности DEX

- Необходимость предпросмотра негативно влияет на производительность симуляции
- Необходимость контролировать SMC
- Переменная длина инструкций усложняет stubbing/patching
- Необходимо контролировать время исполнения гостя
  - А как это делается в многозадачных вытесняющих ОС?
- **Для DEX оптимально иметь аппаратную поддержку на хозяине**

IA-32 virtualization technology (VT-x)



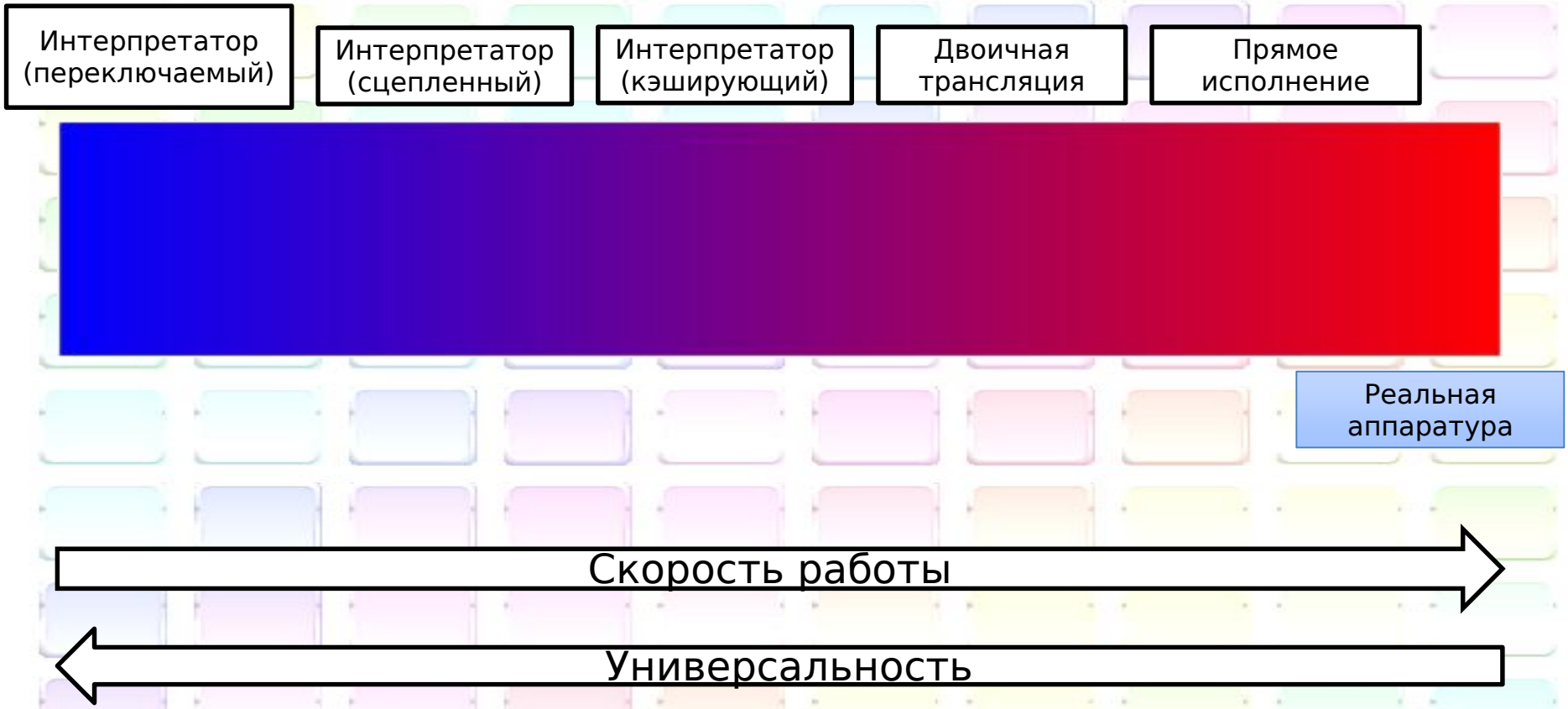
Симулятор, использующий аппаратную виртуализацию

+ Прямое исполнение большинства инструкций
+ Упрощение модели, уменьшение объёма кода симулятора
- Необходима аппаратная поддержка
- Модуль/драйвер ядра
- Медленное переключение между режимами
- Не все режимы процессора могут быть симулированы (например, real mode в IA-32)
- Рекурсивная виртуализация?

Практическое использование VTx

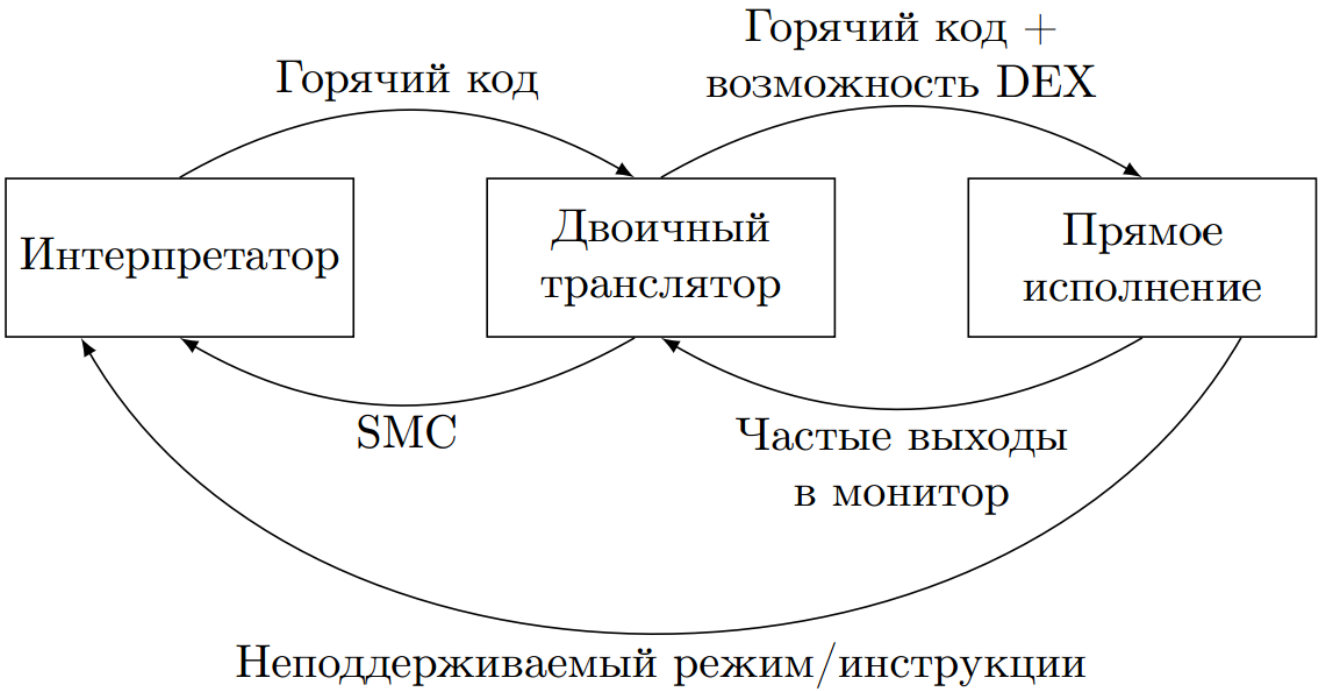
- VirtualBox — VTx необходим для симуляции 64 битных гостей
- Microsoft VirtualPC — VTx необходим
- Wind River Simics — VTx опционален
- VMware ESXi — VTx необходим для симуляции 64 битных гостей
- KVM — VTx опционален
- Xen — VTx очень желателен

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 нескольких симуляторов

Итоги

- Наивное прямое исполнение
- Заплатки и заглушки
- DEX с аппаратной поддержкой
- 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/