Перспективы применения детерминированнго воспроизведения работы виртуальной машины при решении задач компьютерной безопасности

Довгалюк П. М.
Фурсова Н. И.
Дмитриев Д. С.
Новгородский государственный университет

План доклада

- Детерминированное воспроизведение работы виртуальной машины
- Применение детерминированного воспроизведения
- Поддержка нового оборудования в виртуальной машине

Актуальные проблемы

- Многократная отладка сложных ошибок без ручного повторения действий пользователя
  - Поиск ошибок с утечками и порчей памяти, сложно повторяемых, требующих наличия окружения и т.п.
  - Поиск ошибок в драйверах и компонентах ОС
- Реверсивная отладка
  - Возврат к коду, вызывающему ошибку, из кода, где ошибка проявляется
- Снятие трассы выполнения программы
  - Длительная фиксация работы системы
  - Влияние средств трассировки на работающую систему

Детерминированное воспроизведение

- Записывается работа программы при заданных входных данных
- Воспроизведение гарантирует тот же порядок выполнения инструкций, что и при записи
- Подходы к детерминированному воспроизведению:
  - С использованием специальных аппаратных средств
  - Программные реализации
    - Воспроизведение отдельной программы
    - Воспроизведение работы целой системы

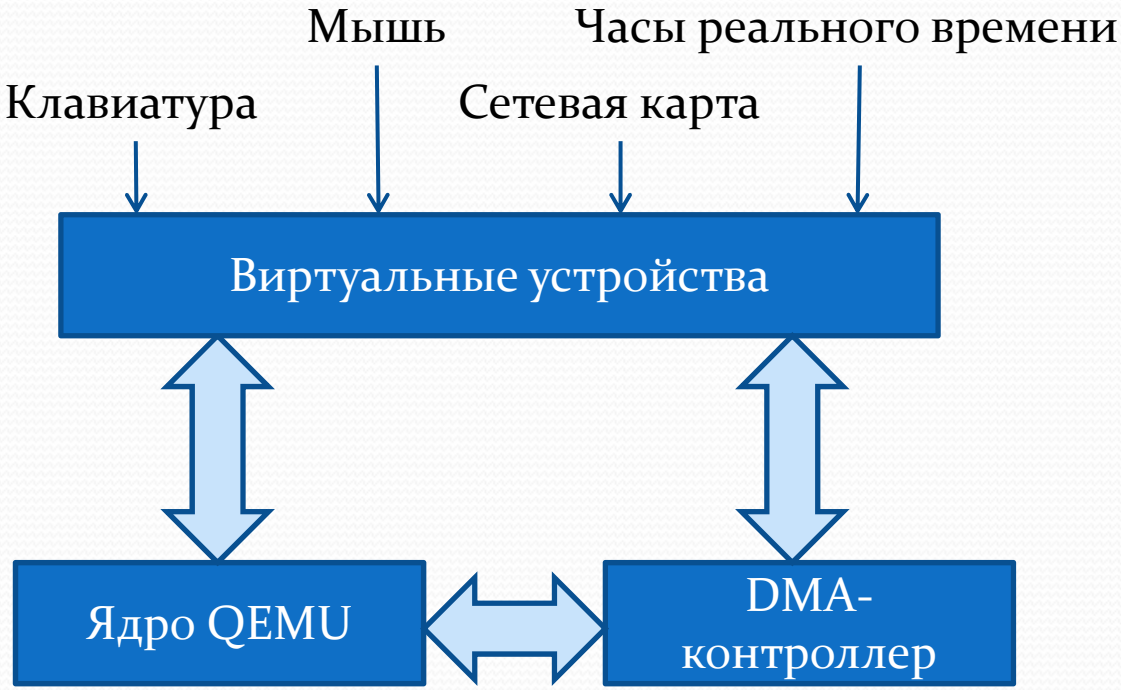
Существующие реализации

- Воспроизведение отдельных программ
  - Реализации: iDNA, PinPlay, Respec, DoublePlay, ODR
  - Каждая из систем ориентирована на конкретную ОС и аппаратную платформу
  - Невозможен анализ компонентов операционной системы (драйвера, библиотеки)
- Воспроизведение системы целиком
  - ReVirt, XenLR, Aftersight – основаны на виртуализации
    - Поддержка только x86
  - ExecRecorder – основан на симуляторе Bochs
    - Поддержка только x86
    - Работает значительно медленнее, чем другие реализации
  - FREE – реализован на основе QEMU
    - Поддержка только x86
    - Отсутствует поддержка DMA-транзакций
    - Исходный код не опубликован

Симулятор QEMU

- Открытый исходный код
  - Можно добавить механизмы для записи/воспроизведения работы виртуальной машины
  - Возможно расширение перечня поддерживаемых платформ и периферии
- Динамическая трансляция
  - Быстрее, чем симуляция инструкций (Bochs), но медленнее, чем виртуализация (Xen, KVM)
- Поддержка различных платформ
  - x86, ARM, MIPS, PowerPC, …

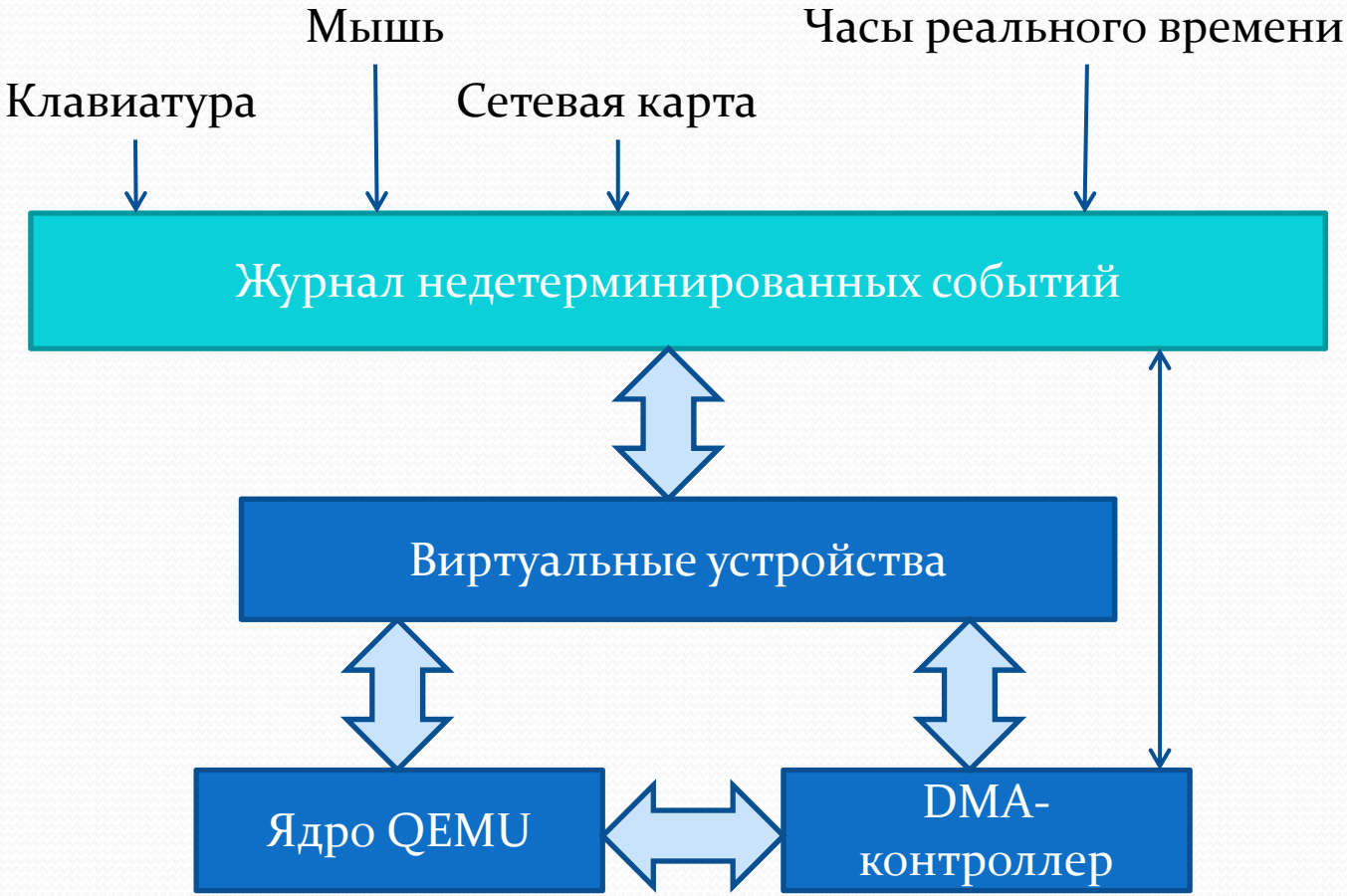
Архитектура QEMU



Подходы к реализации воспроизведения

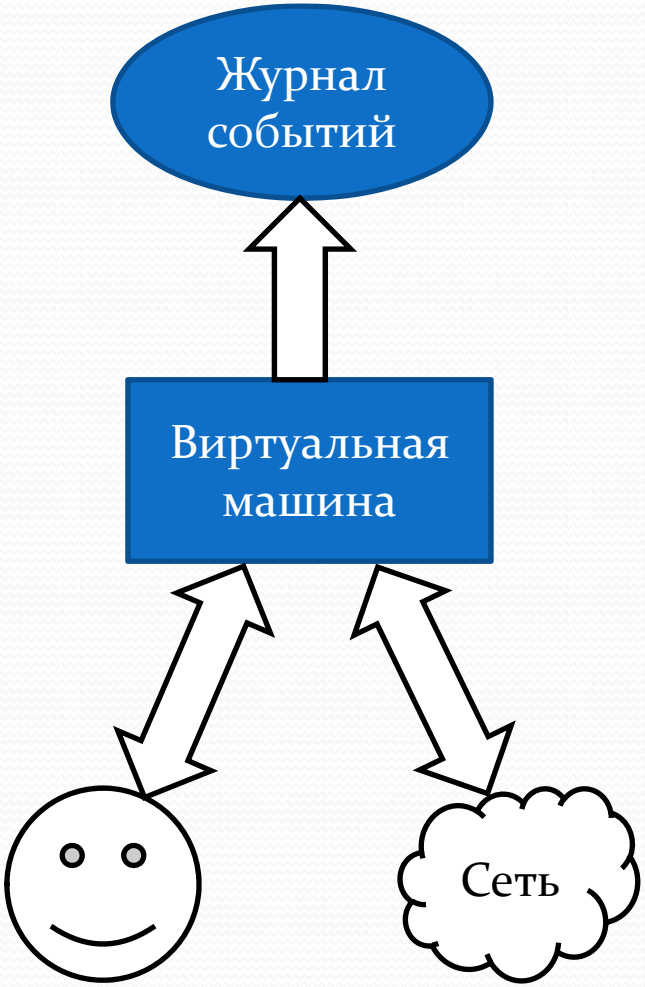
- Записываются результаты всех операций ввода-вывода и работы с памятью
  - Про воспроизведении легко восстановить значения ячеек памяти и регистров
  - Сложно восстановить состояние устройств ввода-вывода (например, флаг статуса контроллера IDE)
- Записываются внешние по отношению к виртуальной машине события
  - При воспроизведении значения ячеек памяти и регистров восстанавливаются с помощью выполнения тех же инструкций, что выполнялись при записи
  - Записывается небольшой объем данных, что оказывает меньшее влияние на анализируемую систему

Воспроизведение работы виртуальной машины



Использование детерминированного воспроизведения

- Запись сценария работы для последующего анализа
  - Взаимодействие с пользователем, сетью и т.п.



Использование детерминированного воспроизведения

- Воспроизведение сценария
  - Анализ выполняющихся программ
  - Может выполняться многократно с повторением достигнутого при записи результата

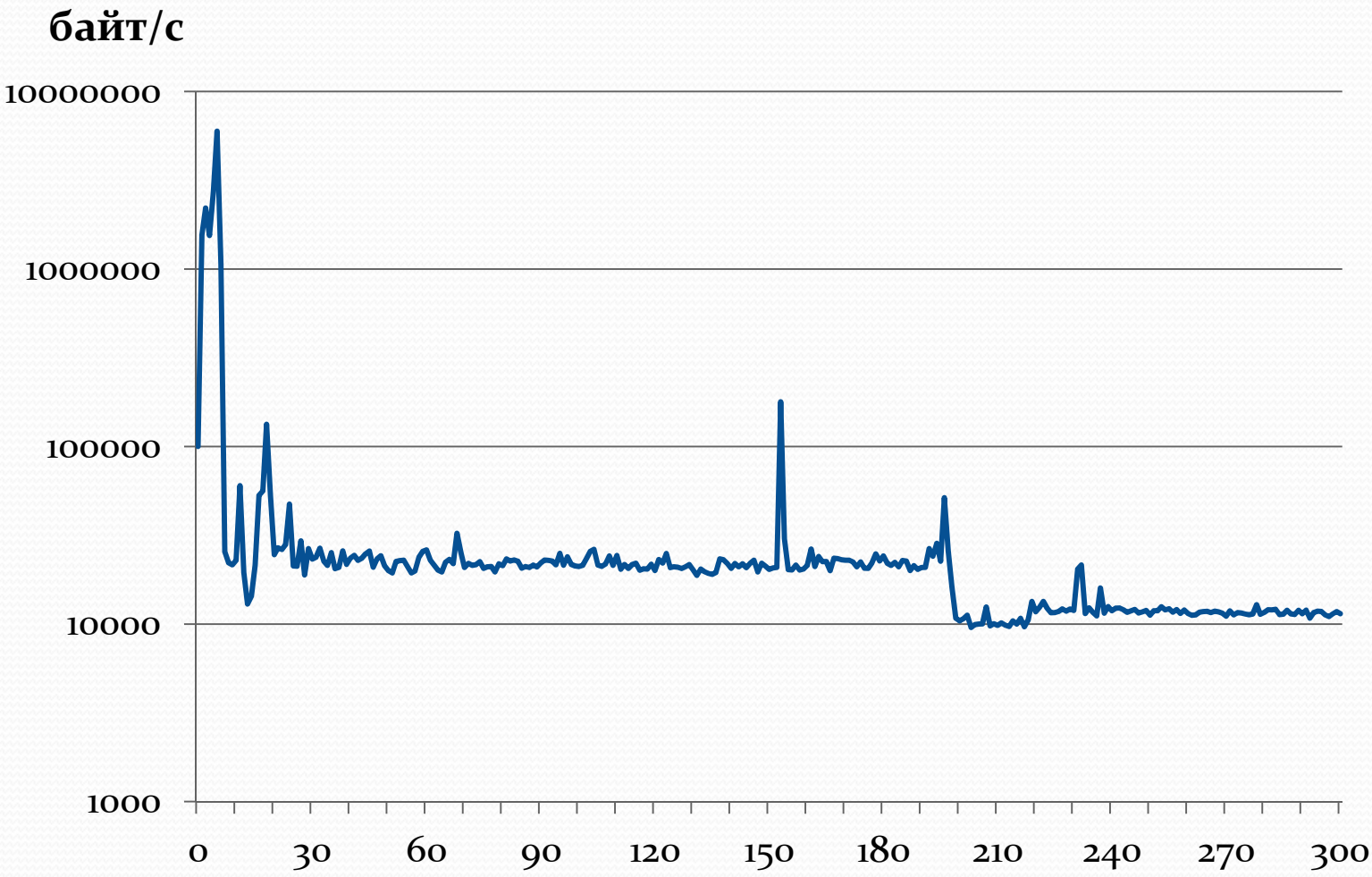
Поддерживаемые платформы и устройства

- Платформы
  - x86/x86_64
    - Linux
    - Windows XP
    - Windows 7
  - ARM
    - Linux
- Периферийные устройства
  - Сетевая карта
  - Мышь
  - Клавиатура
  - Аудиоадаптер

Детерминированное воспроизведение

- Скорость роста журнала – 12 кб/с
- Замедление при записи – 3x
- Замедление при воспроизведении – 14x

Скорость роста журнала



Процесс загрузки Windows XP

Трассировка

- Трасса – последовательность выполненных инструкций и значений регистров на каждом шаге
- Снятие трассы выполняется за два прохода вместо одного

1 проход

Работа пользователя с VM и одновременное снятие трассы

2 прохода

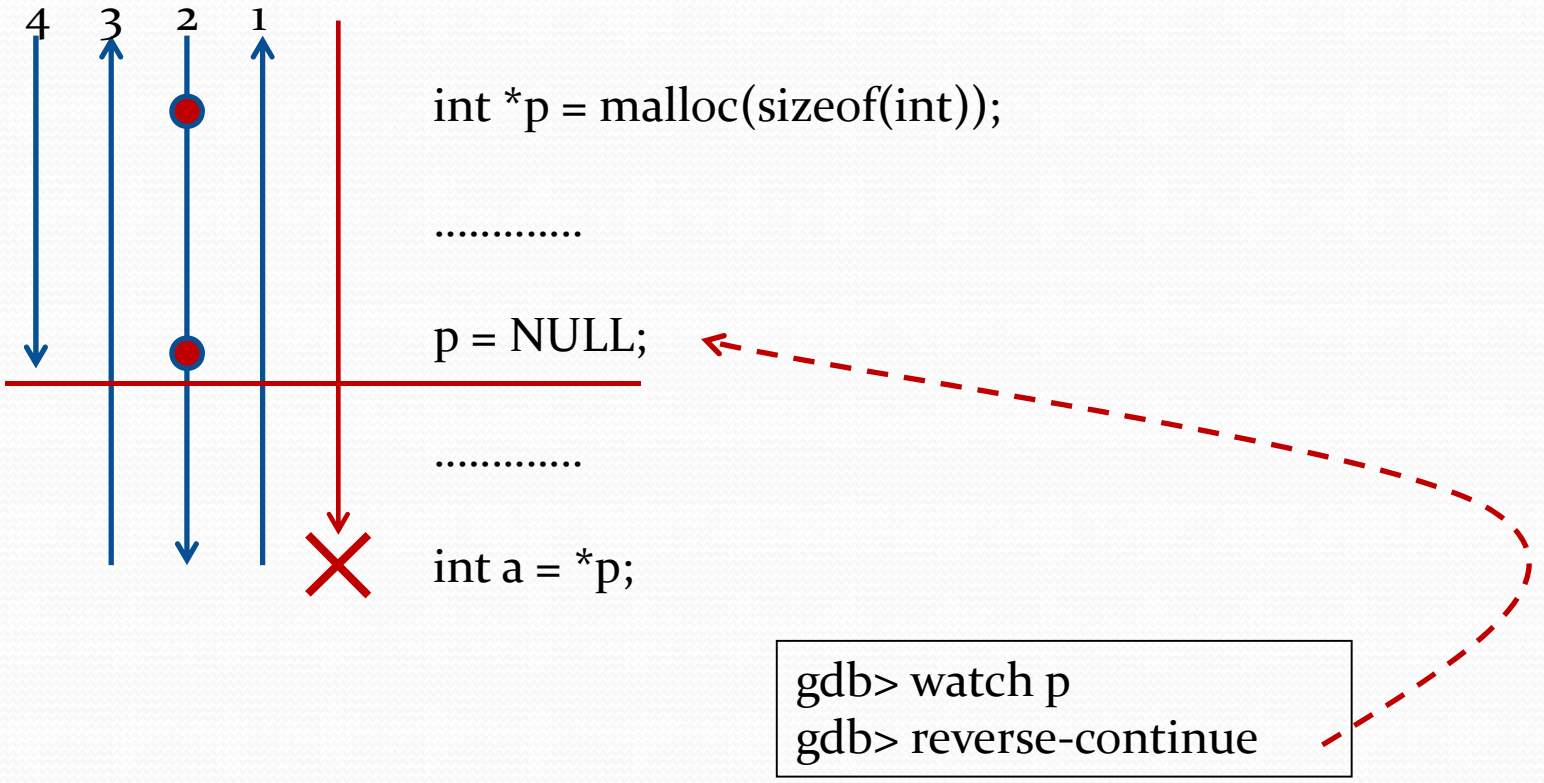
Работа пользователя с VM

Автоматическое снятие трассы при воспроизведении работы VM

Детерминированная отладка

- Работает через интерфейс GDB
  - Пошаговая отладка
  - Переход к произвольному шагу
  - Обратная отладка
- Использует записанные ранее снимки состояния виртуальной машины для быстрого перехода назад

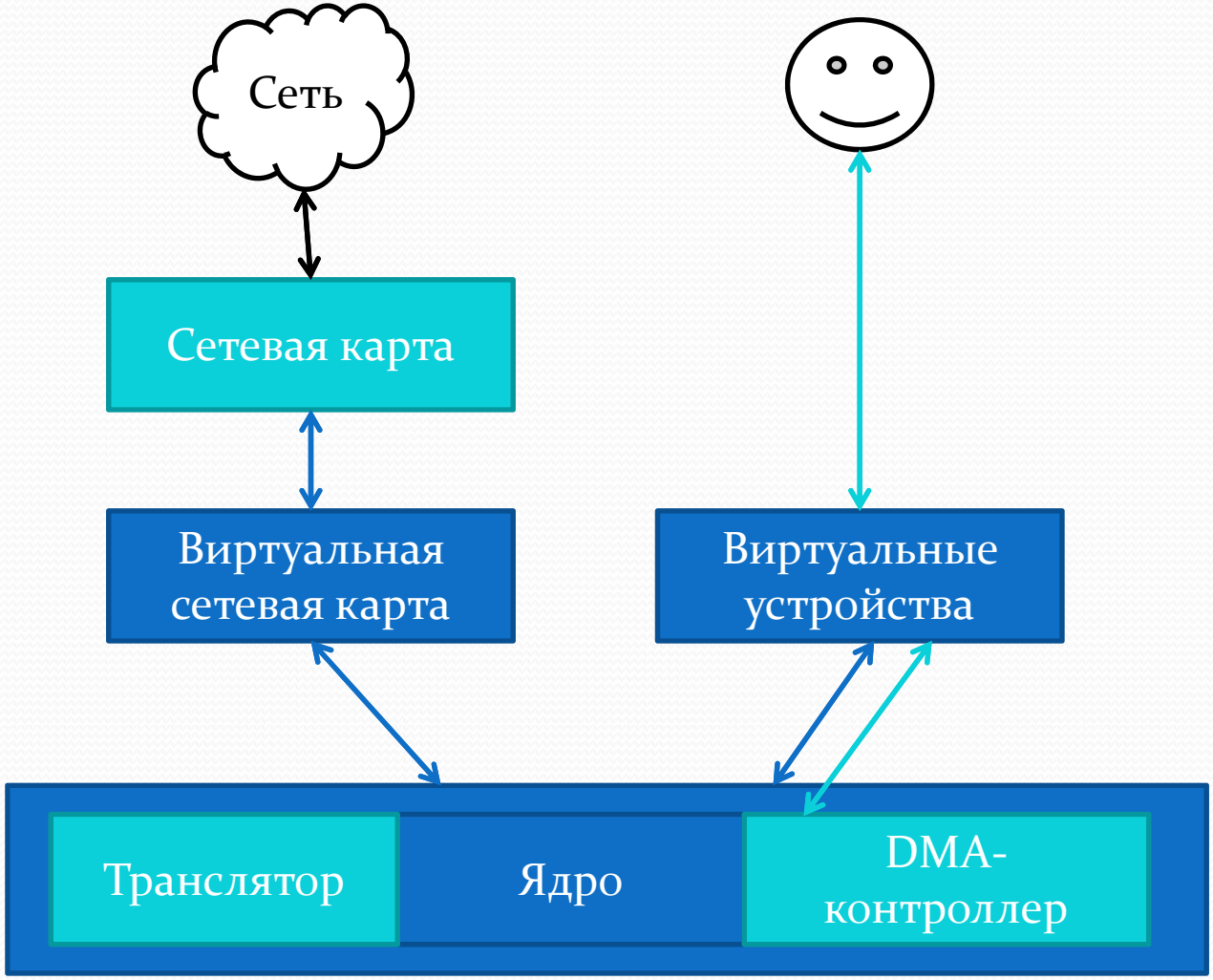
Обратная отладка



Анализ ПО

- Возможен анализ программ, работающих с сетью, за счет применения двухпроходной трассировки
- Использование виртуальной машины в качестве honeypot
  - Объем записываемых данных – 1Гб/сутки (без учета сетевых пакетов)
  - Возможность использования виртуальной машины в реальном сетевом окружении

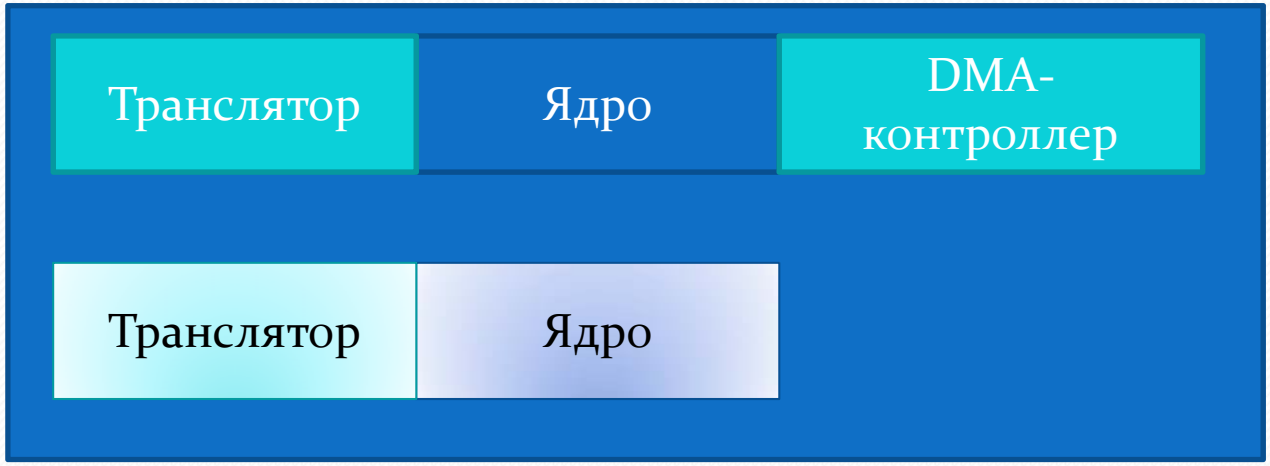
Поддержка детерминированного воспроизведения внутри компонентов симулятора



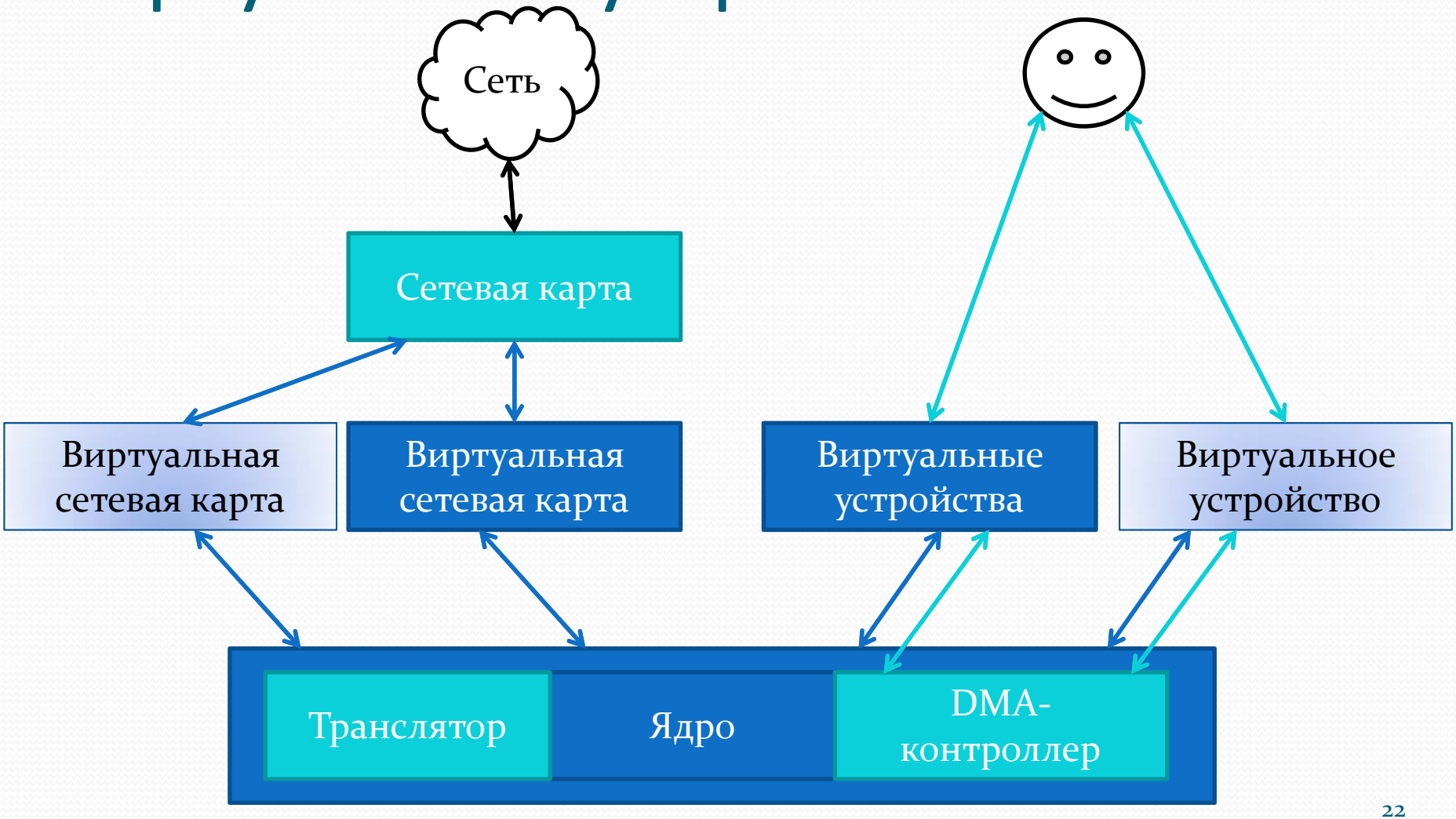
Реализация поддержки новых платформ

- Процессорное ядро
  - Добавление поддержки нового процессора
  - Добавление поддержки расширений для существующего процессора
- Виртуальные устройства
  - Добавление устройств, взаимодействующих с внешним миром
  - Добавление внутренних виртуальных устройств

Расширение симулятора: процессор



Расширение симулятора: виртуальные устройства



Расширение симулятора: трудоемкость

- Поддержка детерминированного воспроизведения для новых устройств:
  - Виртуальное устройство: 1-2 человеко-недели
  - Сетевая карта: 0 человеко-недель
  - Процессорное ядро: 2 человеко-недели
  - Расширение процессора: 1 человеко-неделя

Выводы

- Реализованы возможности для анализа работы виртуальной машины
  - Платформы x86 и ARM
  - Работа в реальном сетевом окружении
- Сравнительно небольшой объем записываемых в журнал данных
  - Возможно длительное наблюдение за работой системы
- Замедление работы при использовании механизмов записи/воспроизведения работы системы сравнимо с аналогичными реализациями

Направления дальнейшей работы

- Воспроизведение работы виртуальной машины с электронными ключами, подключаемыми через USB
- Расширение перечня поддерживаемых симулятором платформ и устройств (маршрутизаторы, мобильные устройства)
- Распараллеливание работы симулятора
  - Ускорение симуляции на многопроцессорных компьютерах
  - Поддержка полноценной симуляции многопроцессорных систем