Разработка методов контейнерной виртуализации для платформы Android

Выполнил: Карташов А. А.
Руководитель: Кринкин К. В.

Кафедра математических и информационных технологий
Санкт-Петербургский Академический университет

2012

Цель

Разработать методы контейнерной виртуализации для платформы `Android`.

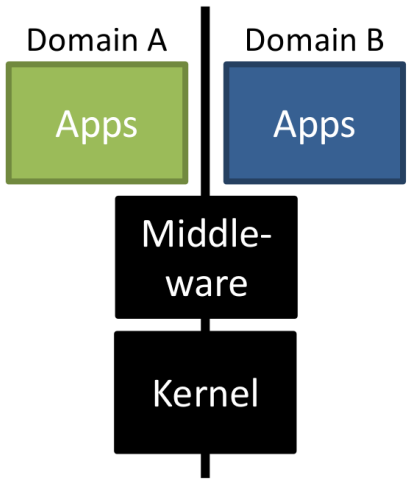
Задачи

- Адаптация LXC для работы на мобильном устройстве.
- Разработка механизма межконтейнерного взаимодействия.
- Обеспечение совместного доступа параллельно работающих контейнеров к
  - драйверам, специфичным для Android: Binder, Alarm.
  - устройствам ввода,
  - телефонии.

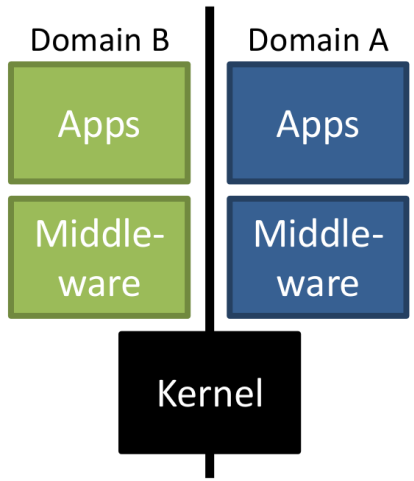
Мотивация проекта AndroidVM

- Большое количество вирусов для ОС Android
  - Для подозрительной программы отдельный Android.
  - Без важной информации.
  - Без возможности отправки SMS.
- Уязвимость корпоративных приложений на смартфоне сотрудника
  - Для корпоративных приложений отдельный Android.
  - Без возможности что-либо установить.

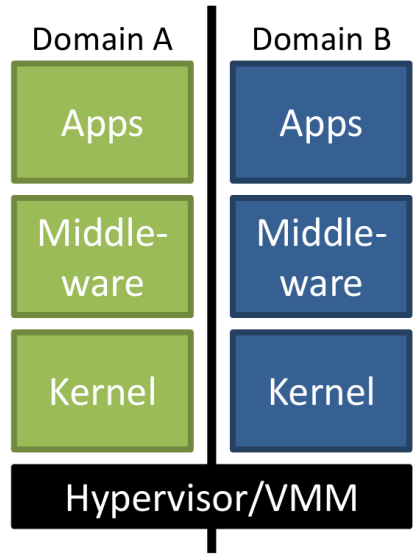
Подходы к виртуализации на мобильных платформах



TrustDroid

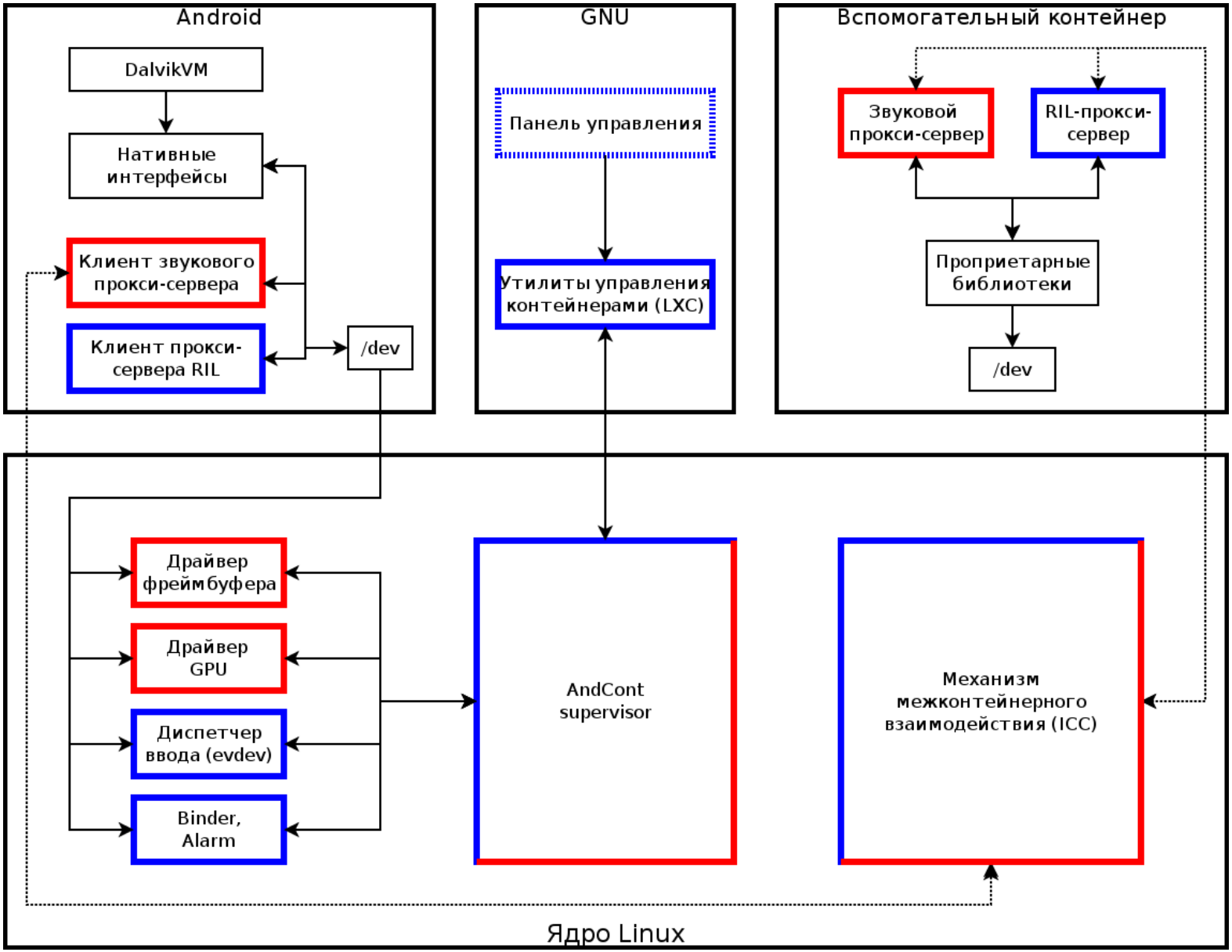


OpenVZ,
Cells



VMWare

Архитектура



Пространства имен ядра

Наборы объектов ядра, которые являются уникальными с точки зрения пользовательского приложения. Пользовательское приложение не может получить доступ к не принадлежащим ему наборам таких объектов через API, экспортируемый ядром.

В ядре Linux пространствами имен являются множества

- идентификаторов процессов,
- точек монтирования,
- сетевых интерфейсов и сокетов,
- объектов IPC,
- идентификаторов пользователей.

Механизм межконтейнерного взаимодействия

Проблема

В ядре отсутствует механизм для взаимодействия между пространствами имен:

- сокеты не работают, т. к. привязаны к сетевому пространству имен,
- пайпы работают, но требуется промежуточный агент в корневом пользовательском окружении.

Решение

Собственный механизм IPC на базе Netlink, в котором отсутствуют изолирующие проверки.

Утилиты LXC (Linux Containers)

Набор утилит LXC — основа для создания виртуальных окружений:

- предоставляет доступ к инфраструктуре пространств имен ядра,
- позволяет ограничивать ресурсы для контейнеров (через файловую систему `cgroup`),
- позволяет ограничивать доступ контейнеров к устройствам.

Проблема

LXC не рассчитан для работы в корневом пользовательском окружении и не позволяет запускать контейнер с окружением Android.

Драйверы, специфичные для ядра Android

Драйверы, препятствующие запуску нескольких пользовательских окружений Android

- Binder — система IPC,
- Alarm — интерфейс к RTC.

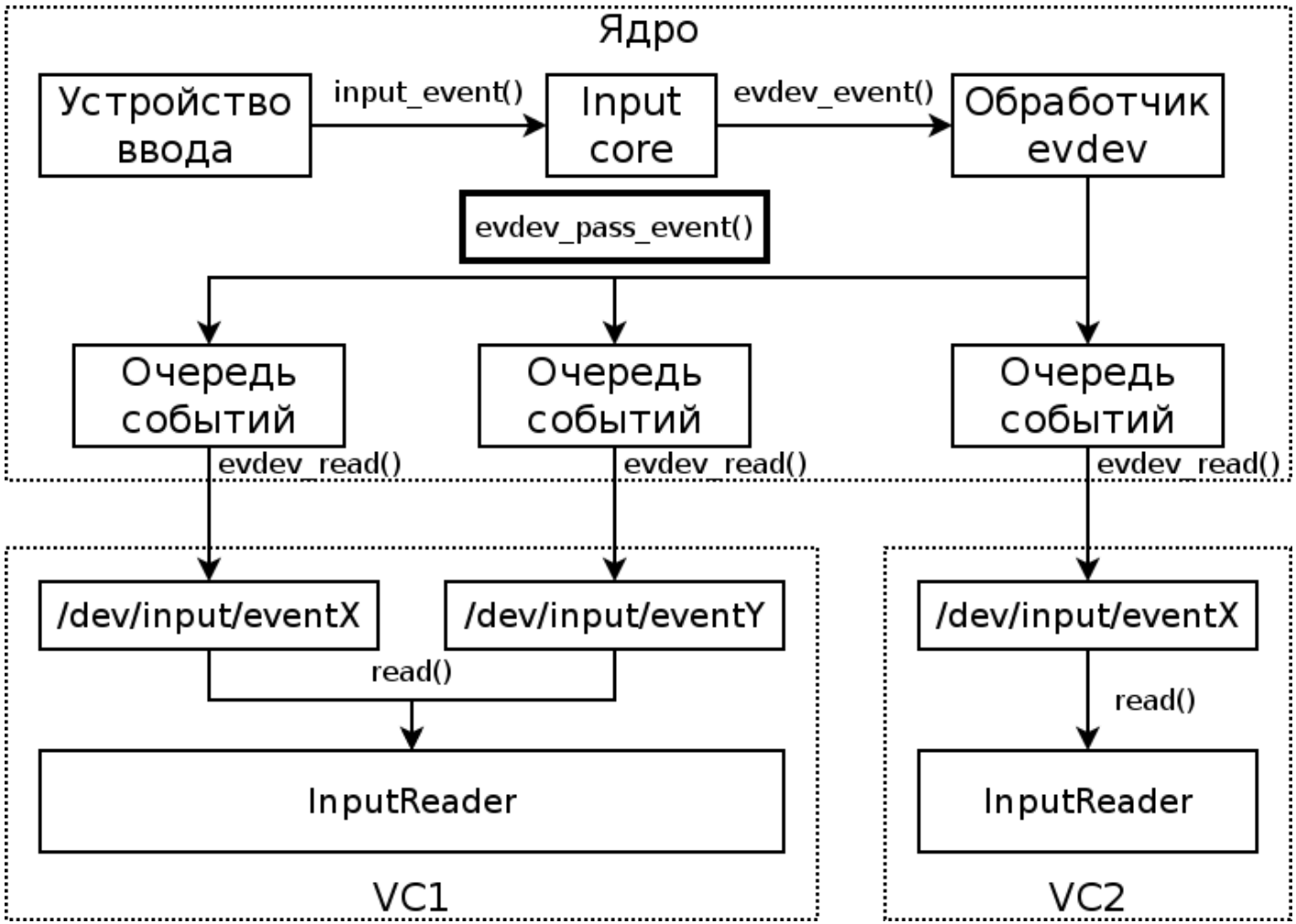
Проблема

Наличие однократно инициализируемого состояния.

Решение

Создание экземпляра состояния драйверов для каждого контейнера.

Архитектура виртуализации подсистемы ввода



Телефония

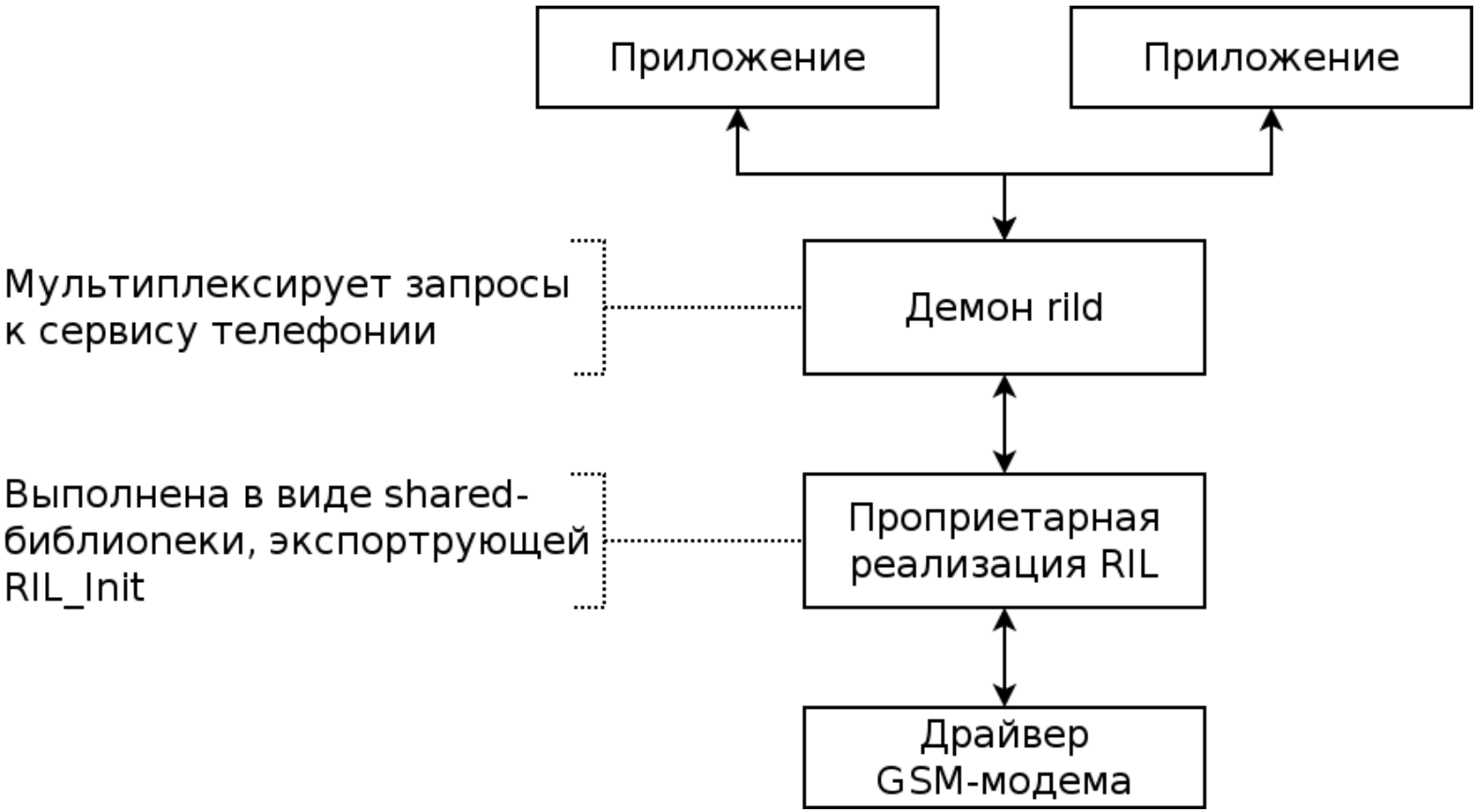
Интерфейс RIL — абстрактный интерфейс доступа к аппаратуре мобильных сетей. Содержит

- запросы с подтверждением,
- асинхронные уведомления,
- синхронные запросы.

Задачи

- маршрутизация входящих SMS и звонков,
- управление исходящими SMS и звонками.

Архитектура стека RIL



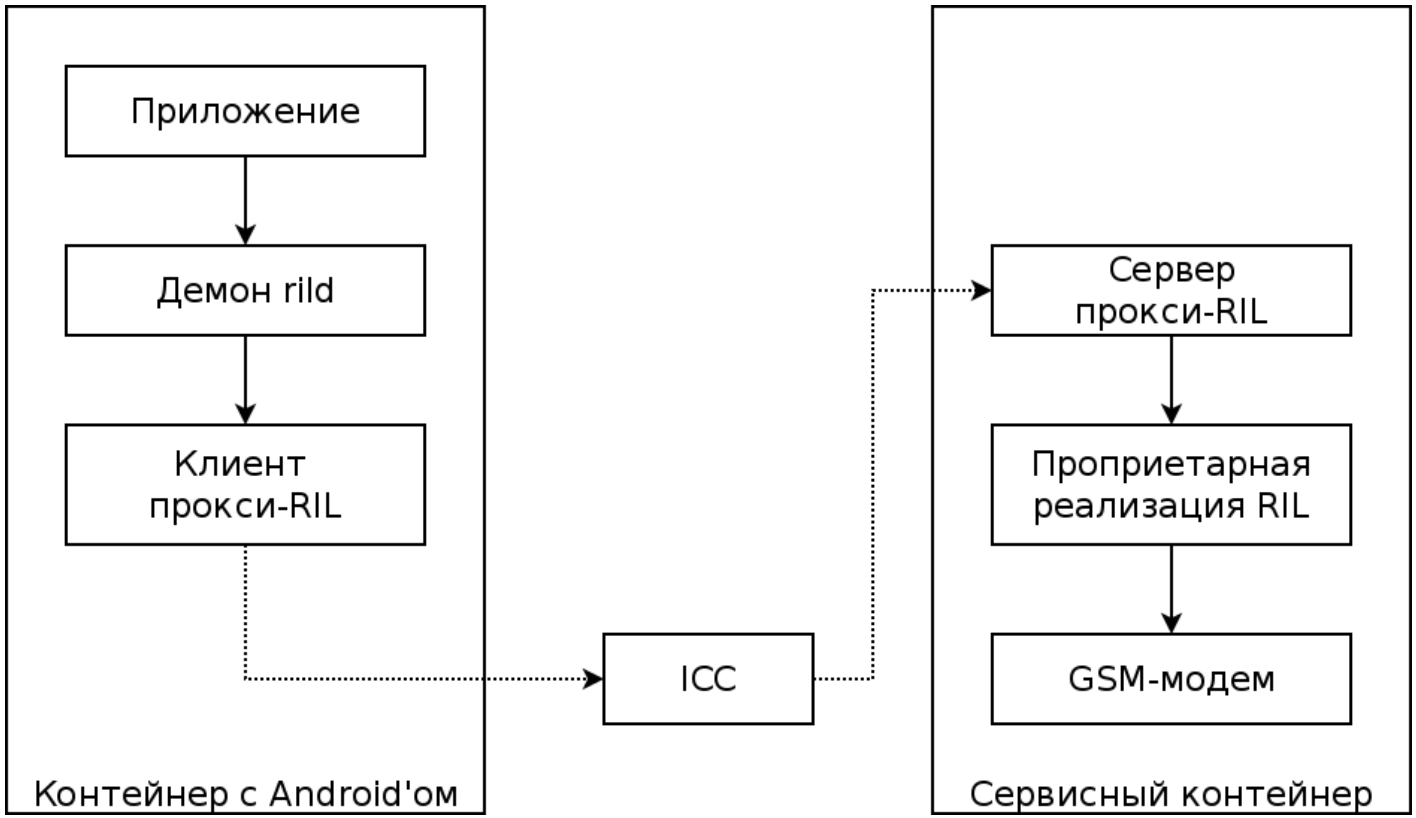
Проблема

Невозможен совместный доступ к GSM-модему из разных контейнеров.

Виртуализация RIL

Решение

Разработка прокси-RIL — разделение интерфейса RIL на клиентскую и серверную части.



Политики мультиплексирования RIL

- запросы с семантикой Get перенаправляются в проприетарную библиотеку безусловно,
- запросы, связанные с отправкой звонков и SMS, разрешены только для активного контейнера,
- асинхронные уведомления, связанные со входящими звонками и SMS, маршрутизируются только в активный контейнер,
- остальные асинхронные уведомления маршрутизируются во все контейнеры.

Результаты

Разработана технология контейнерной виртуализации для платформы Android, которая позволяет

- позволяет запускать несколько окружений Android,
- позволяет переключаться между запущенными контейнерами,
- предоставляет совместный доступ к сервисам RIL и устройствам ввода для всех запущенных контейнеров.

Видео

1. запущены два Андроида,
2. переключаемся в первый и играем в AngryBirds,
3. переключаемся во второй Андроид, включаем музыкальный плеер, переключаемся в контрольную панель,
4. переключаемя в первый контейнер и продолжаем играть в AngryBirds — музыка из второго Андроида продолжает звучать,
5. приостанавливаем AngryBirds и звоним — музыка заглушается,
6. звонок завершен — музыка продолжается,
7. возвращаемся во второй контейнер и останавливаем музыку.

Спасибо за внимание!

WiFi

Проблема

- Некоторые приложения (AndroidMarket) требуют активного беспроводного соединения.
- В ядре нет готовых драйверов виртуальных беспроводных интерфейсов.

Решение

Эмулировать состояние беспроводного соединения путем модификации нативной библиотеки Android.

Направления дальнейших работ

- реализация доступа к устройствам,
- управление доступом к сервисам RIL,
- конфигурация беспроводных интерфейсов (WiFi, 2G/3G) в корневом пользовательском окружении,
- поиск способов минимизировать потребление памяти Android'ом.