Новгородский Государственный Университет имени Ярослава Мудрого

Использование ABI для интроспекции виртуальных машин

Н.И. Фурсова
П.М. Довгалюк
И.А. Васильев

Интроспекция

- Получение данных из операционной системы
- Использование для динамического анализа

Задачи

- Получение данных из ОС без знания внутренней структуры
- Анализ систем, в которые невозможно загрузить приложение
- Анализ систем на разных платформах

Существующие подходы

- PinOS
  - Плагины от Pin
  - Xen
- RTKDSM (Real-Time Data Structure Monitoring)
  - Интроспекция
  - Xen, Volatility
- Panda
  - Интроспекция + воспроизведение + taint-анализ
  - QEMU 1.0
- DECAF
  - Интроспекция + taint-анализ
  - QEMU 1.0

Особенности подходов

- Модульная структура
- Получение данных из структур операционных систем
- QEMU 1.0

Использование ABI

- Планировалось добыть все данные из системных вызовов

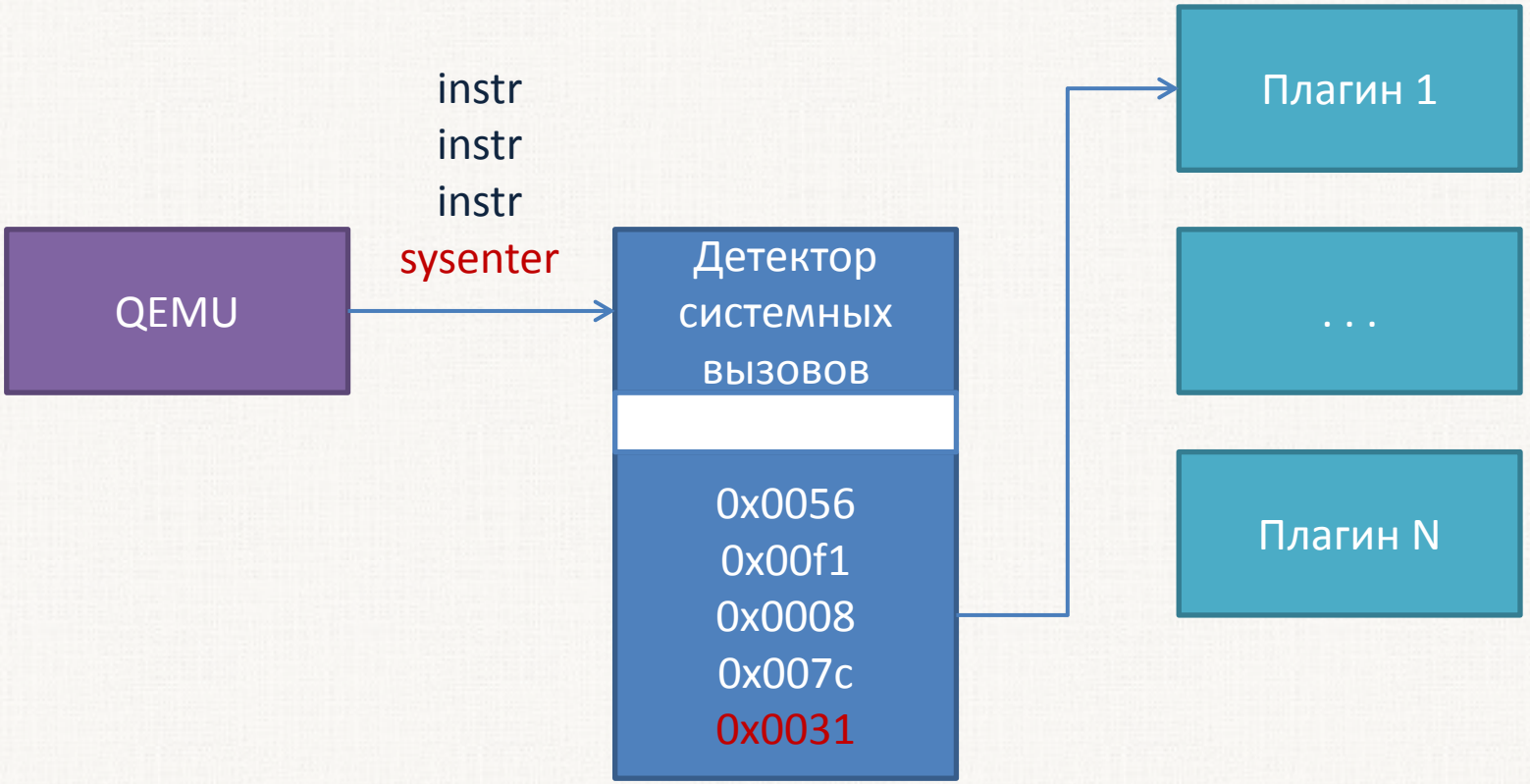
  ABI – Application Binary Interface

- Реализация
  - QEMU
  - Плагины
  - Воспроизведение

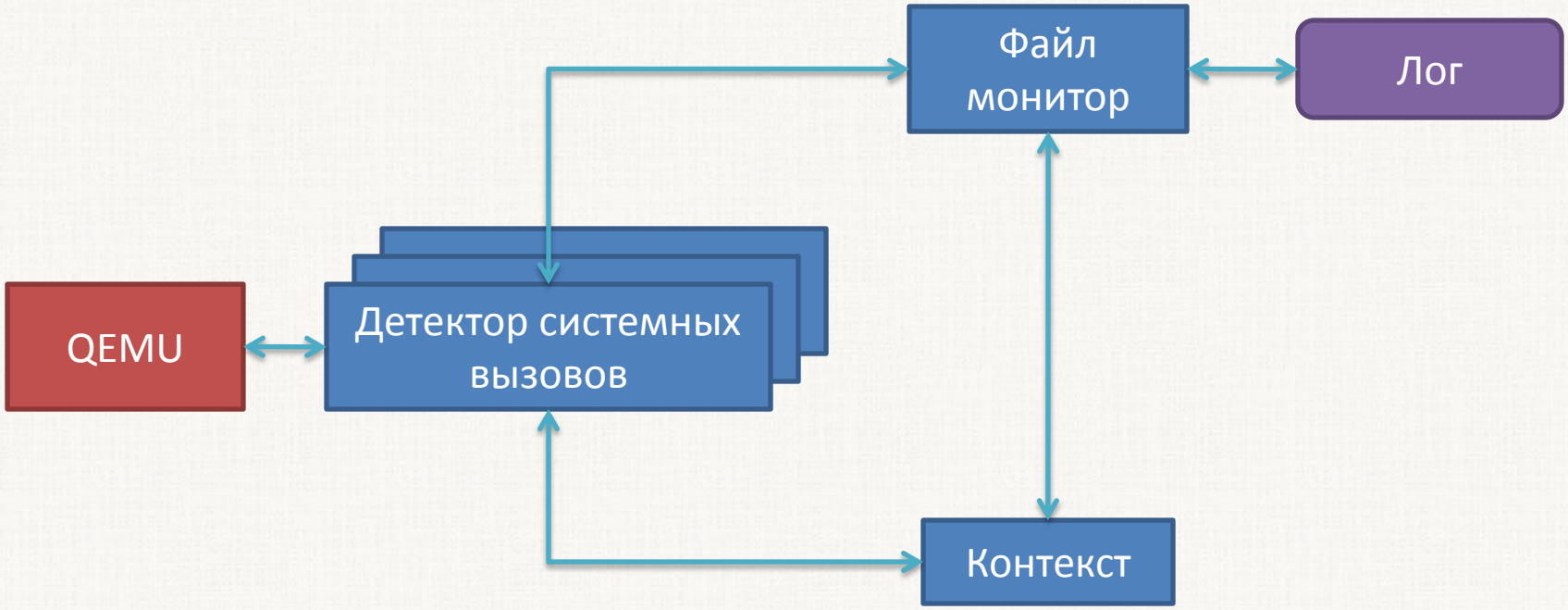
ABI

- Соглашения о вызовах
- fork
- open
- NtOpenFile
- NtCreateProcess

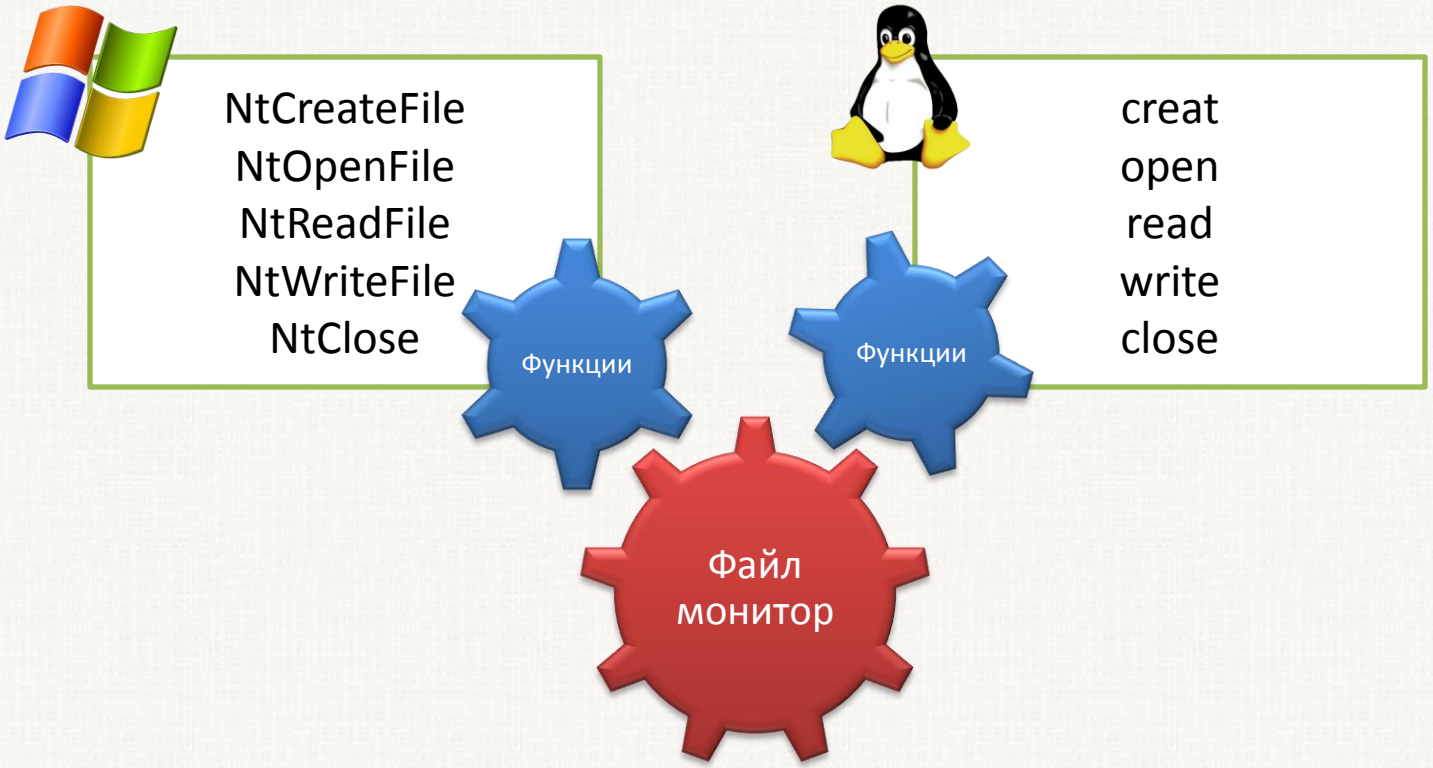
Перехват системных вызовов



Информация о файлах



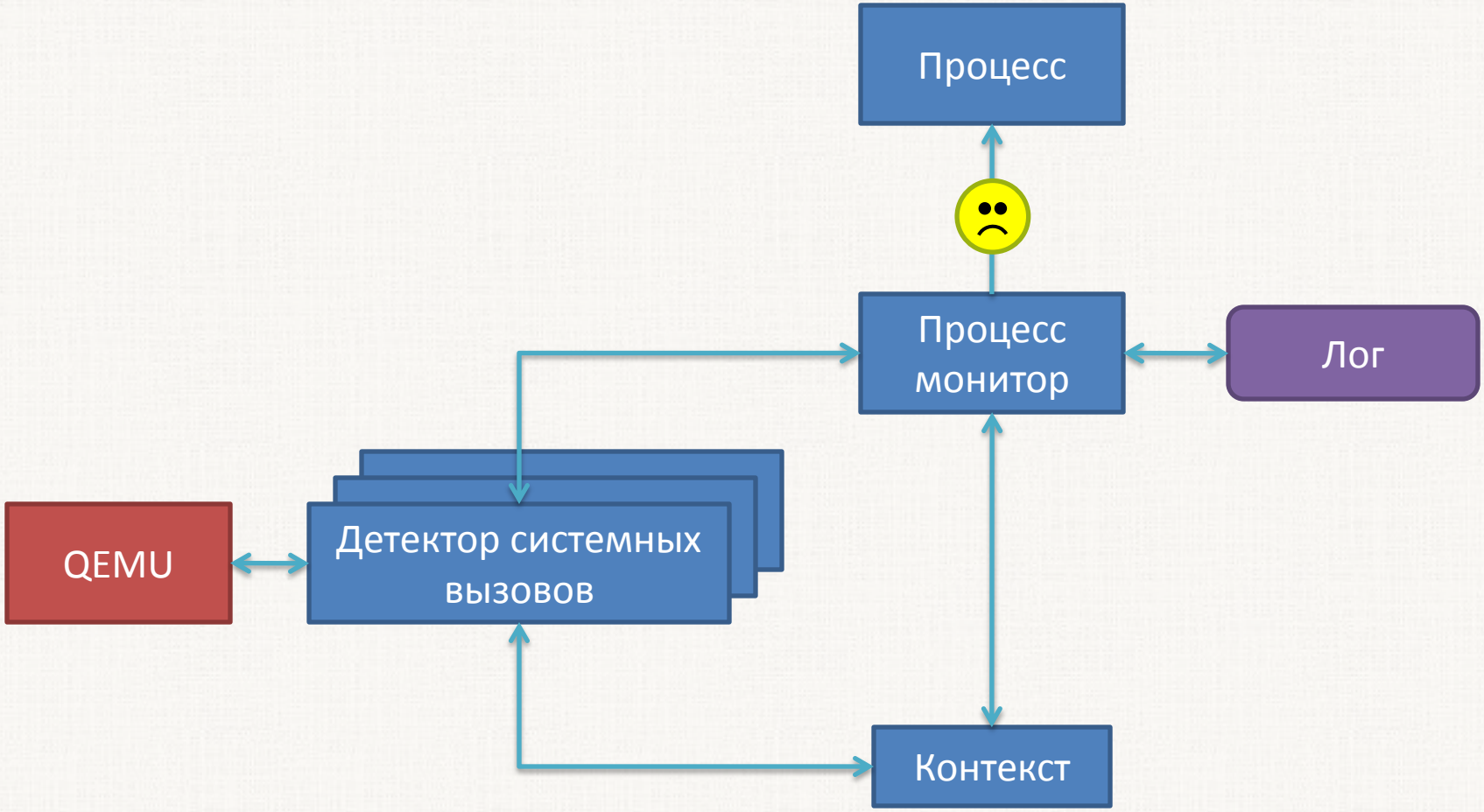
Унификация файл монитора



Абстрактный лог

Платформо-независимый анализ

Информация о процессах



Информация о процессах

- NtCreateProcess (handle)
- NtOpenProcess (*in* ClientID)
- NtTerminateProcess
- NtResumeProcess
- NtSuspendProcess
- NtCreateThread (ClientId)
- NtQueryInfoProcess (ProcessBasicInformation)

Монитор API функций

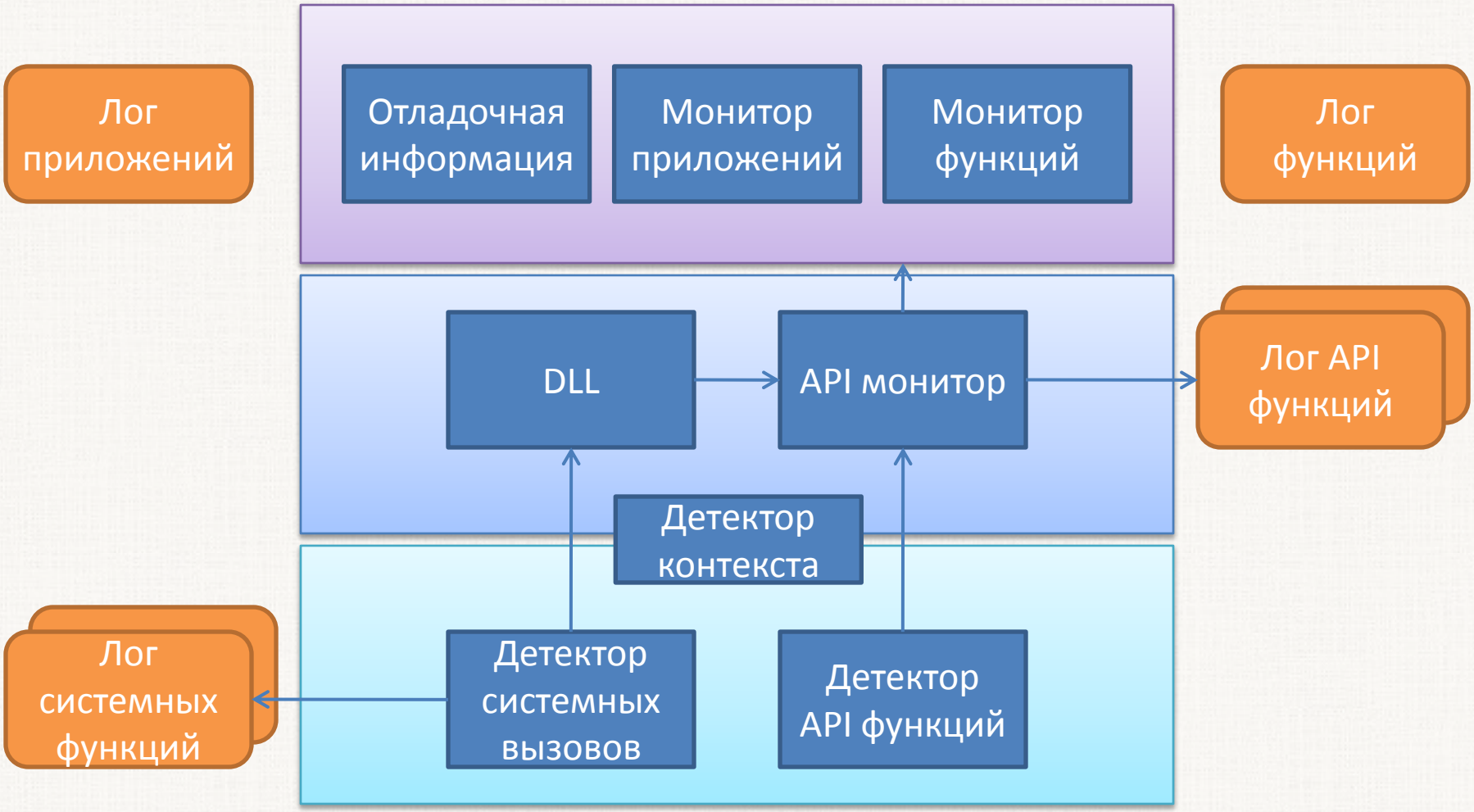
- kernel32.dll
  - Базовый адрес
  - Адрес функции

kernel32.dll

- NtOpenFile (name, fileHandle)
- NtCreateSection (name)
- …
- NtOpenSection (name, sectionHandle)
- NtMapViewOfSection (**baseAddress**)

baseAddress + kernel32.funcAddress = pc

Прототип системы



Результаты

- Подход к интроспекции через ABI
- Файл монитор
- Прототип API монитора