Новгородский Государственный Университет имени Ярослава Мудрого

Легковесный метод интроспекции виртуальных машин

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

Интроспекция

- Получение данных из операционной системы
- Использование для динамического анализа
  - Профилирование кода
  - Обнаружение вредоносного ПО
  - Мониторинг отдельных приложений

Актуальность

- Отладка эмуляции новых платформ
- Анализ вредоносного ПО
- Анализ систем, в которые невозможно загрузить приложение

Традиционный подход

- Внутренние структуры
- Программы-агенты
  - Запускается один раз для считывания информации
  - Работает в системе постоянно
- Учет параметров сборки гостевой ОС

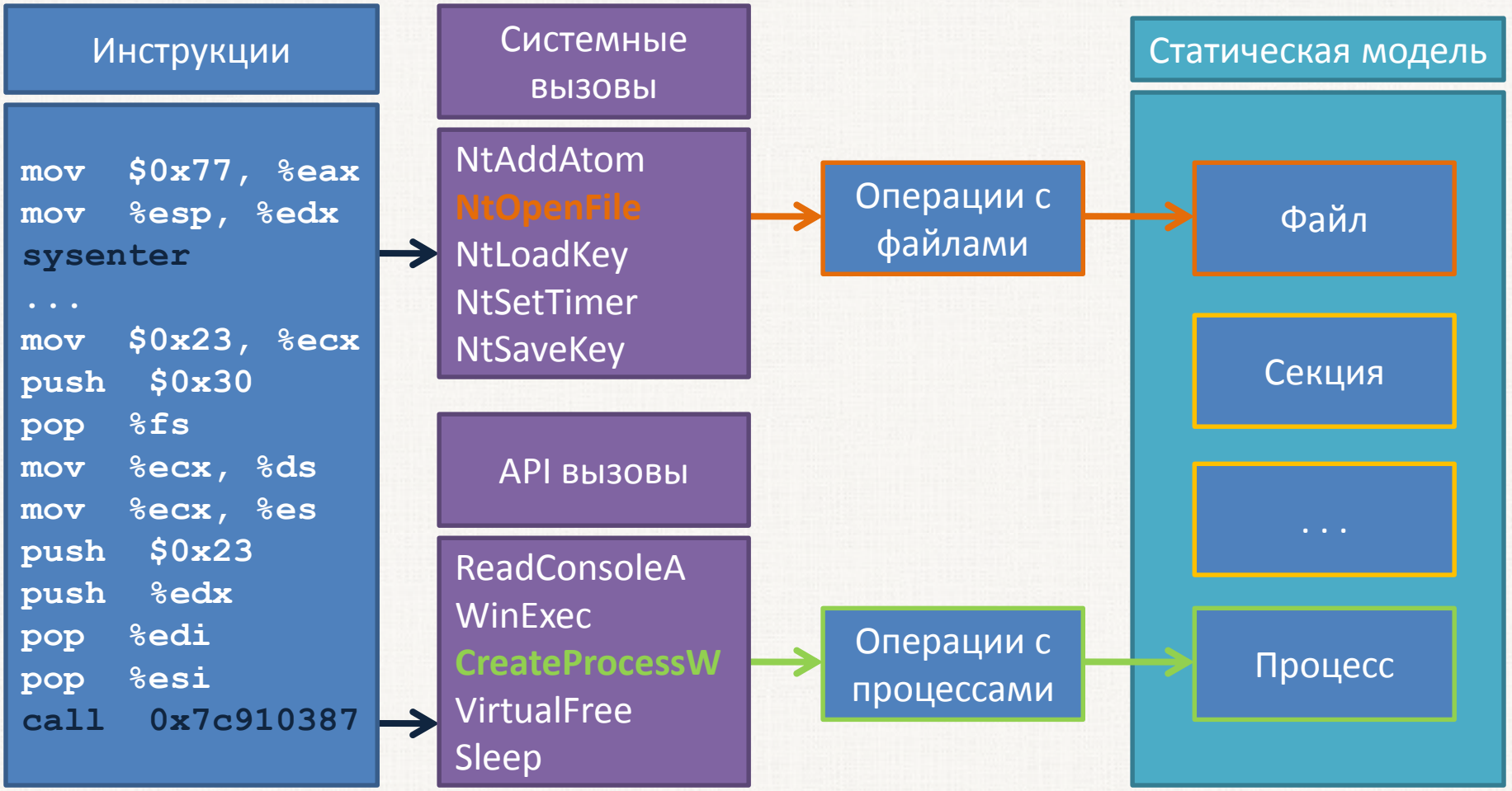
Проблемы

- Плохая переносимость между версиями ОС
- Система в ПЗУ
  - Нельзя загрузить агента
  - Неизвестны версия исходников и параметры сборки
- Невозможность работы агента при воспроизведении записанного сценария

ABI

- Соглашения о вызовах
- Системные вызовы
- Сигнатуры функций
- PE/ELF

Схема работы метода



Файловый монитор

```
NtReadFile(HANDLE  FileHandle, HANDLE Event, PIO_APC_ROUTINE  ApcRoutine,
PVOID ApcContext, PIO_STATUS_BLOCK IoStatusBlock, PVOID  Buffer,
ULONG Length, PLARGE_INTEGER ByteOffset, PULONG Key );
```

```
read(int handle, void *buffer, int nbyte);
```

```
Abstract read(file handle, address of the buffer, number of bytes to read)
```

Create file	Open file	Read file	Write file	Close file
Returned file handle Name of the file File access mode	Returned file handle Name of the file File access mode	File handle Address of the buffer Number of bytes to read	File handle Address of the buffer Number of bytes to write	File handle

Процессы в Linux

pid	Имя образа	Контекст выполнения
-	/sbin/mount	0x359b8000
-	/sbin/mkdir	0x359b8000
0x2a	-	-
-	/sbin/systemd-tmpfiles	0x359b8000
0x2d	-	-
-	-	0x359ff000

	context	pid	image
new_context	+		
fork/clone		+	
execve	+		+
getpid	+	+	

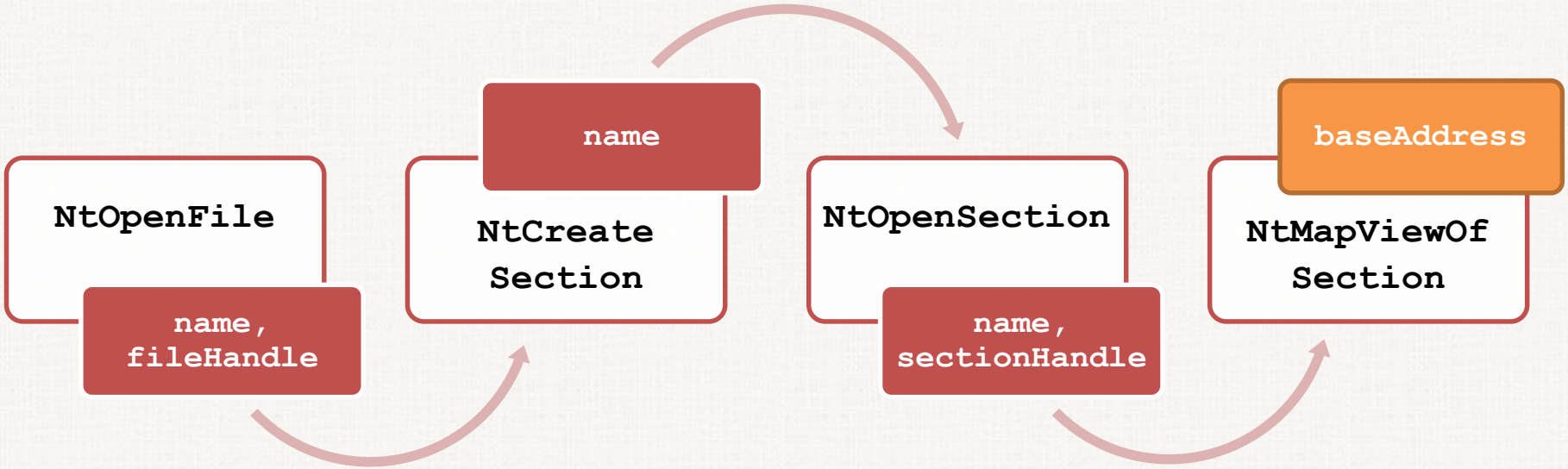
Процессы в Windows

	context	pid	image
new_context	+		
NtCreateProcess			?
NtOpenProcess		+	?
NtCreateThread		+	
NtQueryInfoProcess	+	+	

API

- *.dll / *.so
  - Имя библиотеки
  - Базовый адрес
  - Смещения экспортируемых функций

Обнаружение библиотеки



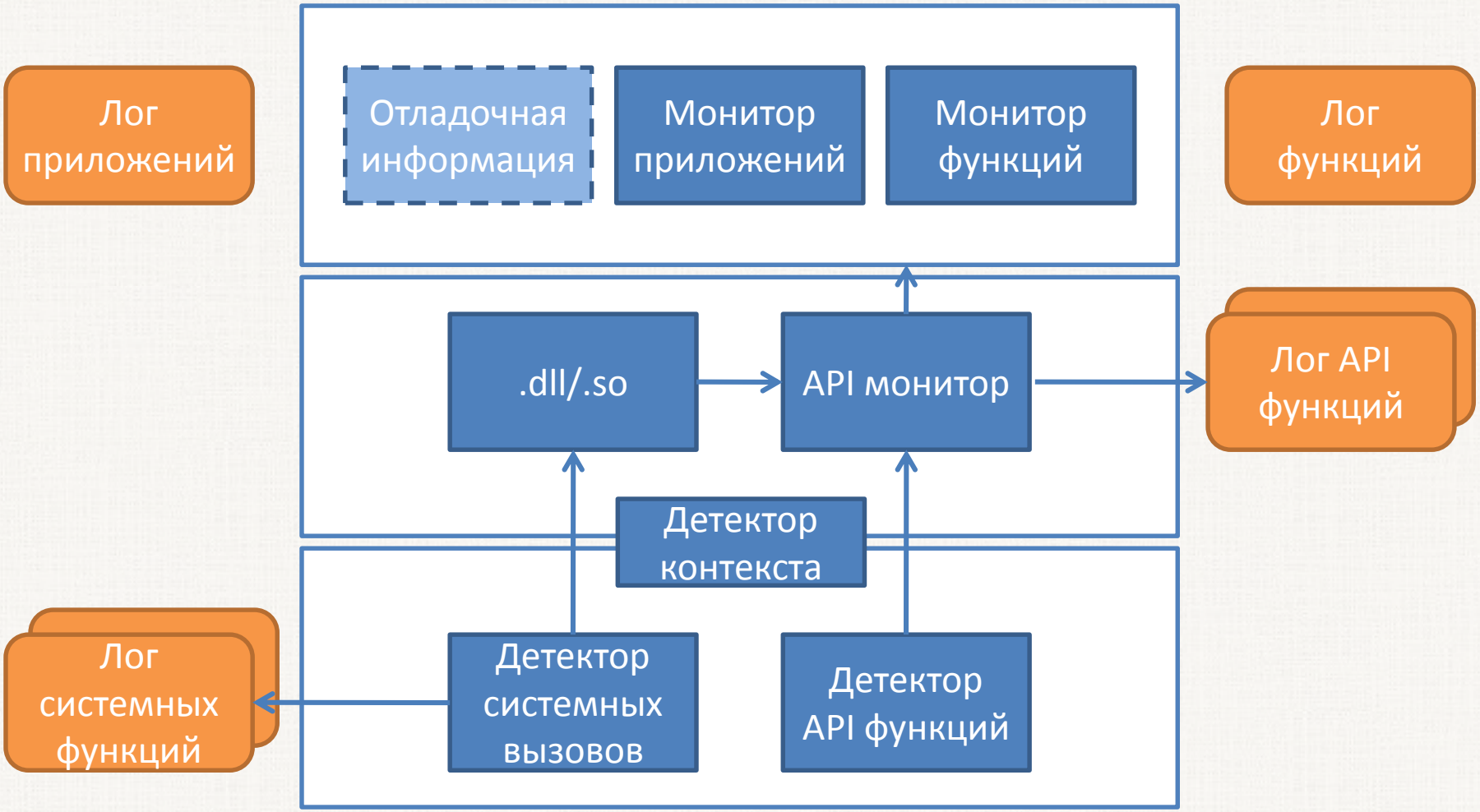
Мониторинг API

- Windows XP, 7, 8
- Linux 2.6 – 4.x
  - Встроенные системы
  - Ubuntu
  - Arch Linux

Список процессов Windows

pid	Имя образа	Контекст выполнения
0x20c	C:\WINDOWS\system32\lsass.exe	0x97b3000
0x2a8	C:\WINDOWS\system32\svchost	0x9a88000
0x2f0	logonui.exe	0x97b3000
0x328	C:\WINDOWS\System32\svchost.exe	0x9a88000
0x4a0	C:\WINDOWS\system32\userinit.exe	0x97b3000
0x568	C:\WINDOWS\system32\wuauclt.exe	0xb45a000
0x614	rundll32.exe	0x9a88000
0x634	C:\WINDOWS\system32\NOTEPAD.EXE	0xb47e000
0x668	C:\WINDOWS\System32\logon.scr	0x97b3000

Структура модулей для QEMU



Результаты

- Метод интроспекции через ABI
- Программный инструмент для создания модулей интроспекции
- Модули для мониторинга:
  - файлов
  - процессов
  - API функций