Получение содержимого удаляемых и изменяемых файлов в среде динамического анализа исполняемых файлов Drakvuf

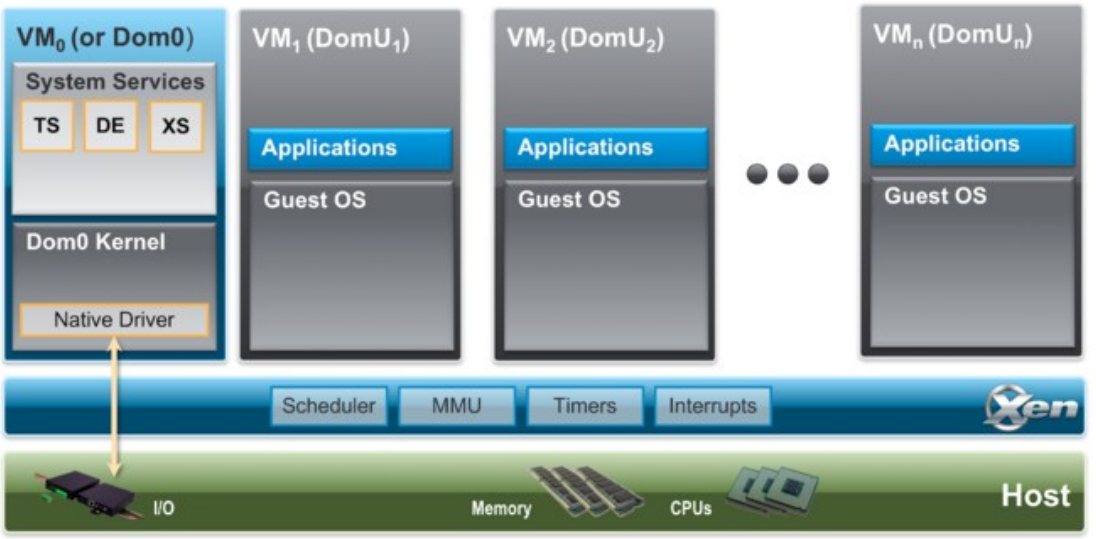
С.Г. Ковалёв <skovalev@ptsecurity.com>
Positive Technologies

План

- Обзор среды:
  - Xen
  - LibVMI
  - Rekall
  - Drakvuf
- Диспетчер кэша
- Инъекция системных вызовов
- Получение файлов
- Заключение

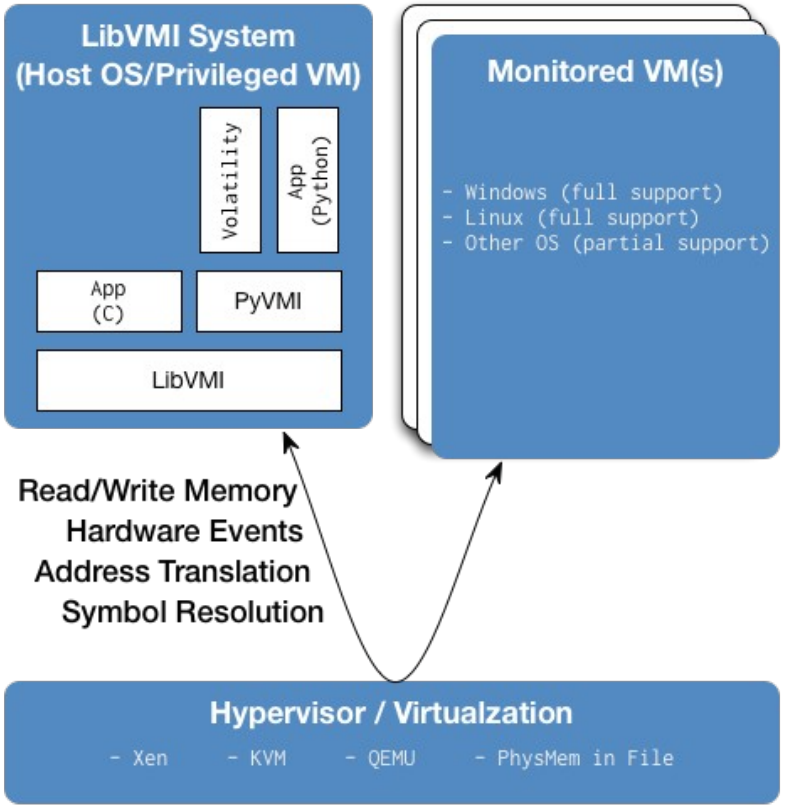
Обзор среды: Xen

- Автономный гипервизор (Тип-1)
- Dom0 — управляющий домен
- DomU — непривилигрованный домен
- Xen 4.5 — *Virtual Machine Introspection* API



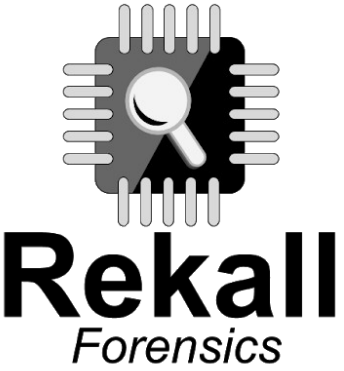
Обзор среды: LibVMI

- Библиотека написанная на Си
- Остановка и запуск ВМ
- Чтение и запись состояния ВМ:
  - память
  - регистры
- Обработка событий ВМ:
  - доступ к памяти
  - изменение контрольных регистров
  - отладочное прерывание (INT3)



Обзор среды: Rekall

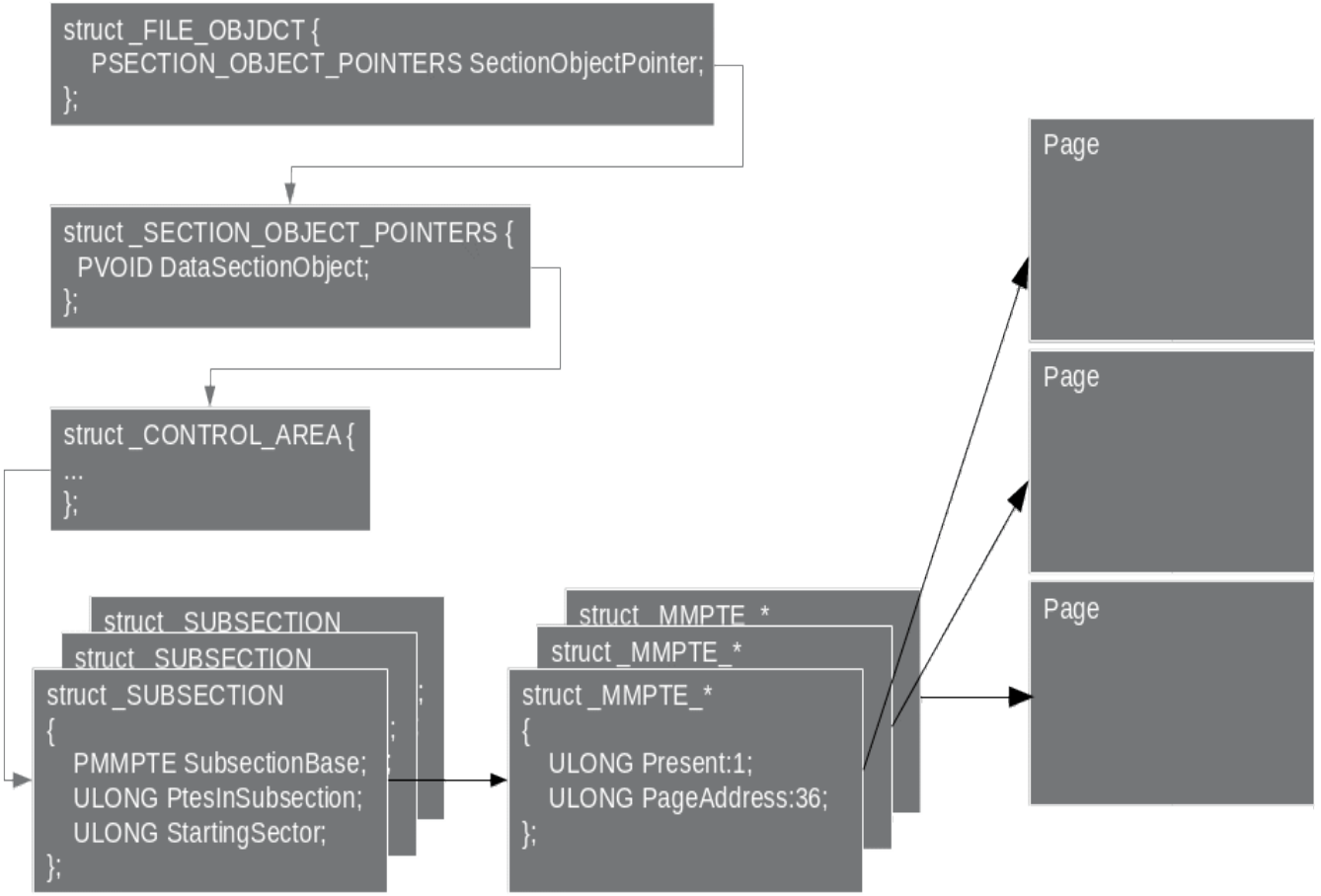
- Среда анализа виртуальной памяти
- Преобразование PDB в JSON:
  - описание модуля (семейство, версия, номер сборки)
  - список символов и их относительные адреса
  - структуры (члены и смещения)
- Позволяет преодолеть семантический разрыв между гипервизором и ядром



Обзор среды: Drakvuf

- Объединяет возможности LibVMI, Rekall и знания о внутреннем устройстве ОС
- Во время обработки выхода из ВМ позволяет:
  - определить текущий процесс и поток
  - определить виртуальный адрес символа
  - установить ловушку на виртуальный адрес
  - получить имя файла по описателю
- Расширяемая архитектура
  - syscalls — отслеживание системных вызовов (ntoskrnl.exe)
  - **filedelete** — отслеживание удаляемых и изменяемых файлов

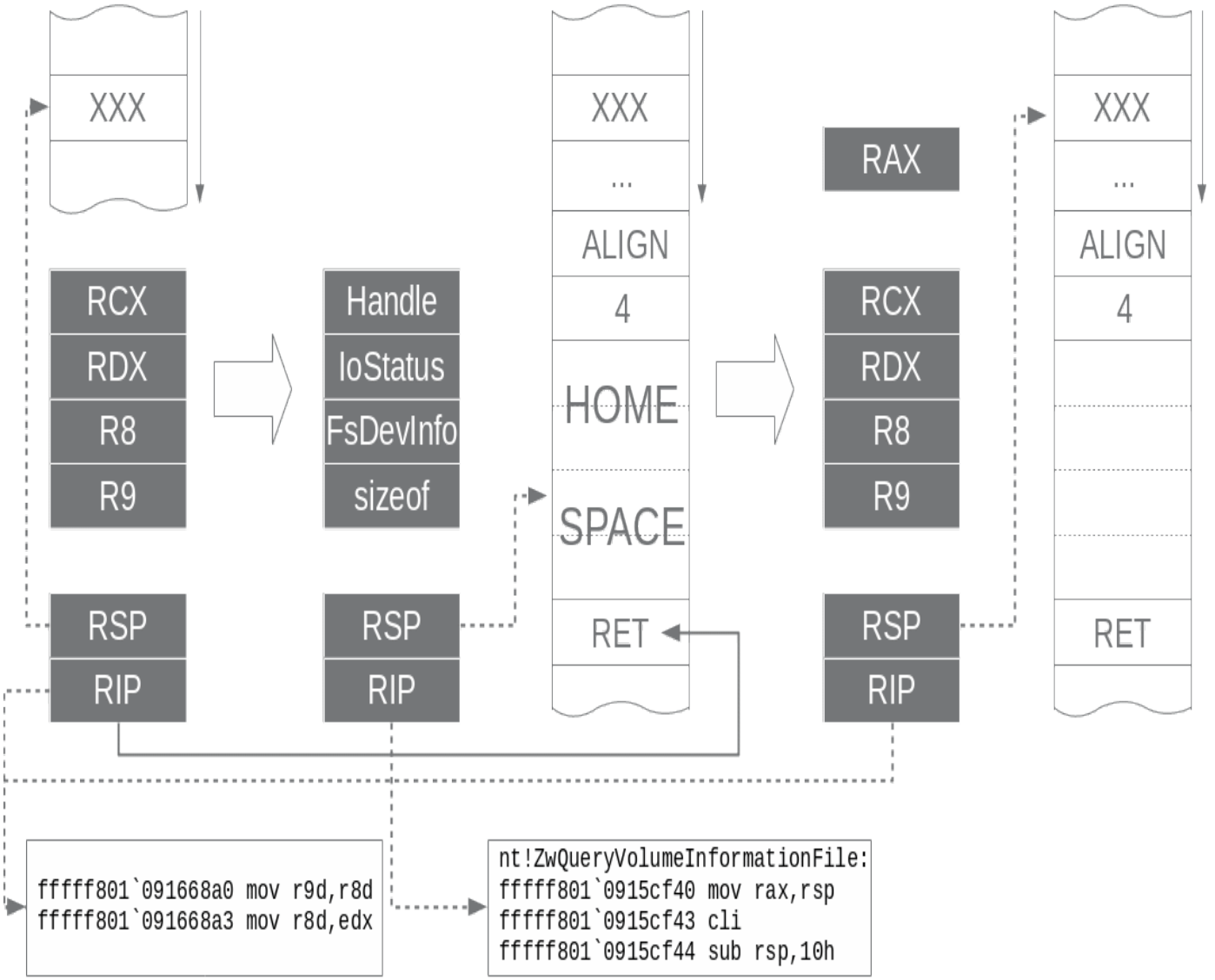
Диспетчер кэша



Диспетчер кэша: ограничения подхода

- Большие файлы загружаются фрагментами
- Данные диспетчера расположены в системном наборе
- Проецируемые в память файлы не поддерживаются

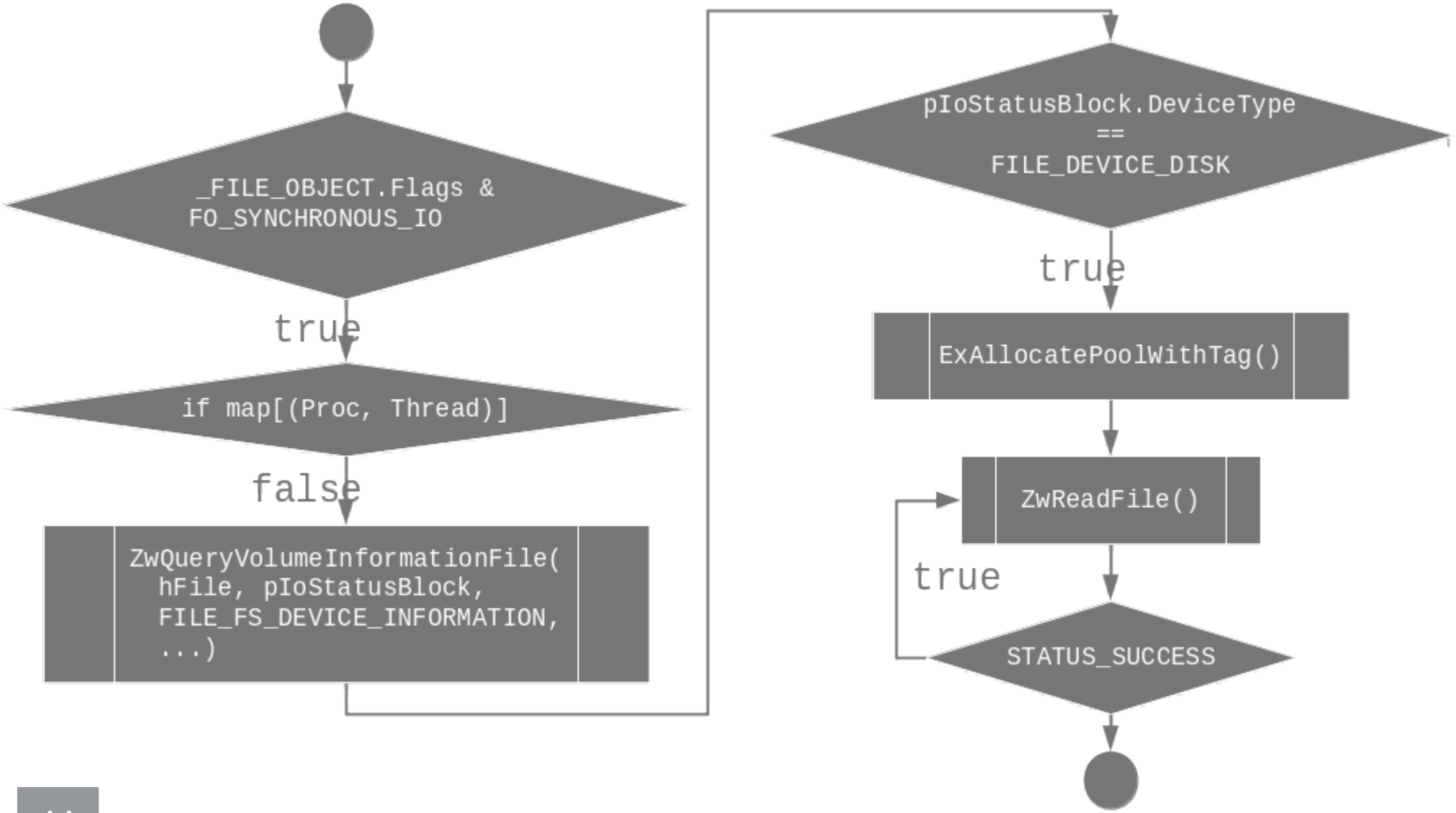
Инъекция системных вызовов



ZwReadFile

- Описатель может быть связан с логическим томом диска, устройством ввода-вывода и т. д.
- Для чтения файлы необходимо подготовить блок памяти достаточного размера
- Для файлов не умещающихся в буфер необходимо несколько вызовов операции чтения
- Чтение асинхронных файлов может приводить к непредвиденным ошибкам

Получение файлов



Заключение

- Достигнуто
  - Использование документированных функций ядра со стороны гипервизора
  - Отсутствие агентских приложений или драйверов
  - Получение содержимого больших файлов
- Дальнейшая разработка
  - Получение содержимого файлов, открытых для асинхронного доступа