Общий подход к восстановлению адресного пространства процесса из образа памяти ОС Android

Свидерский Павел, 545 группа

Научный руководитель: ст. преп. Губанов Ю. А.

Рецензент: ст. преп. Зеленчук И. В.

13 июня 2013

Цифровой криминалистический анализ мобильных устройств

- Мобильные телефоны (смартфоны)
- Планшетные компьютеры
- MP3-плееры
- Электронные книги
- Устройства GPS

Хранят данные о коммуникации и работе в сети

Экспертиза мобильных устройств

- Карта памяти (файловая система)
- Оперативная память
  - Активные приложения (вредоносные)
  - Расшифрованные данные
  - Сетевые соединения

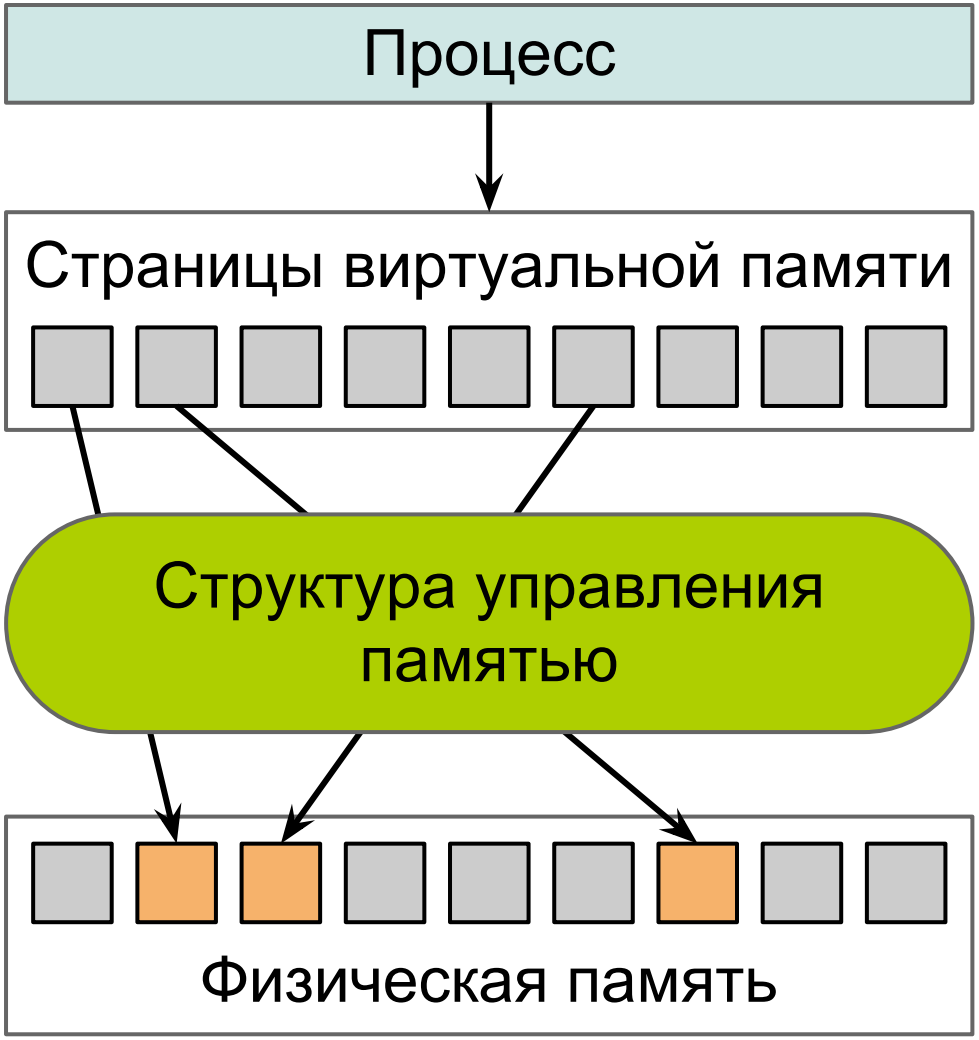
Проблемы:

- Огромное количество моделей устройств, прошивок, версий ОС
- Отсутствие стандартизации интерфейсов

Постановка задачи

- Разработать общий подход к анализу образа оперативной памяти мобильного устройства на базе ОС Android
  - Найти и идентифицировать процессы
  - Восстановить их адресное пространство
  - Не зависеть от версии Android и модели устройства
- Реализовать разработанное решение

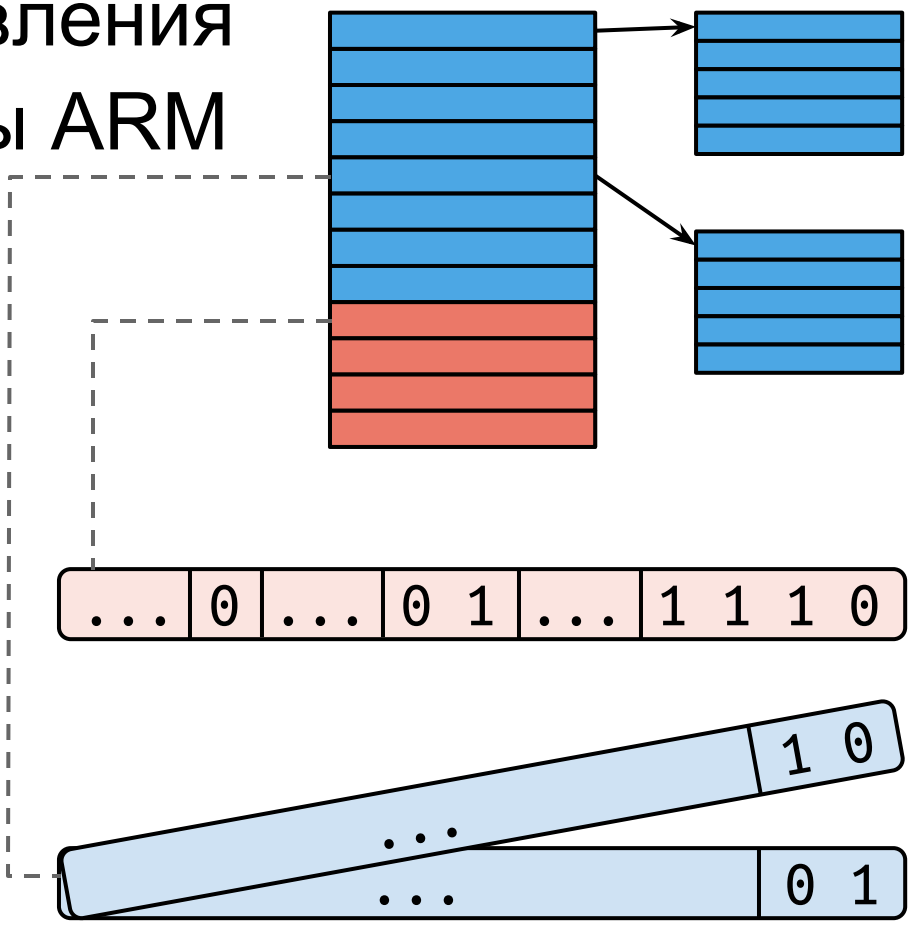
Адресное пространство процесса



Нахождение процессов (1)

Поиск структур управления памятью архитектуры ARM

- сигнатуры
- аппаратные флаги



Нахождение процессов (2)

Поиск структур ядра Linux

- сигнатуры
- эвристики

Определение имён процессов

Восстановление адресного пространства процесса

1. Последовательный обход записей структуры управления памятью
2. Извлечение найденных страниц
3. Запись в файл

- Избавляет от фрагментации памяти
- Позволяет применять стандартные методики поиска данных пользователя в восстановленном пространстве

Результаты

- Разработан общий подход к нахождению процессов в образе памяти мобильного устройства под управлением ОС Android
  - не зависит от версии ОС и модели устройства
  - способно находить скрытые процессы
- Разработан алгоритм восстановления адресного пространства процесса
- Решение реализовано в Volatility Framework (+ тестирование)
- Интегрировано в коммерческий продукт