Мониторинг работы операционной системы в реальном времени на основе гипервизора

Небогатиков Иван
группа 444
научный руководитель: ст. пр. Ханов Артур Рафаэльевич
рецензент: Воробьева Алиса Андреевна

КОДА

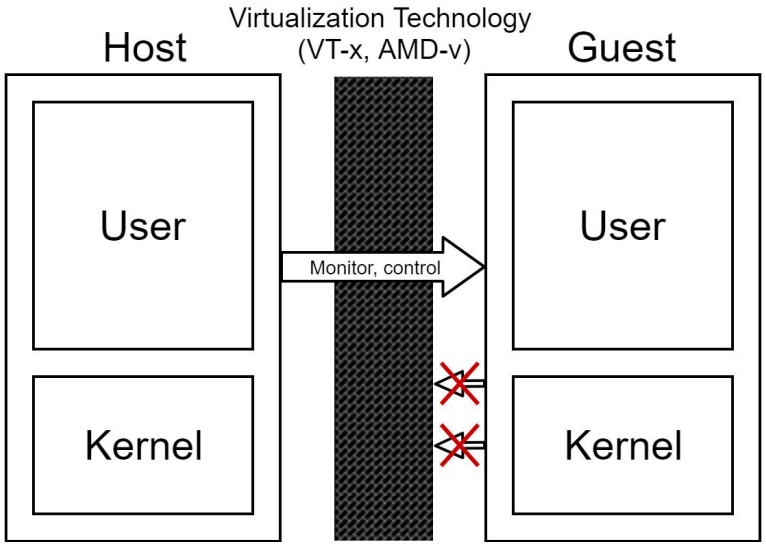
- Изучает поведение программ, установленных на компьютере и фиксирует аномалии в их поведении
- Она блокируется Kernel patch protection
- Нет самозащиты
  - Файлов на диске
  - Процессов

Задачи

- Создание системы самозащиты для антивируса КОДА
  - Перехватчики системных вызовов
  - Файлы на диске
  - Процессы
- Тестирование производительности

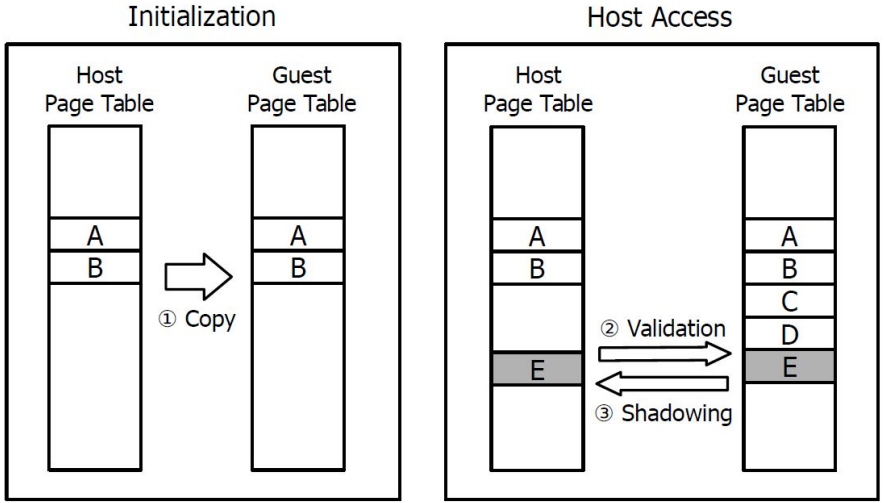
Виртуализация

- Поддерживается современными процессорами
- -1 кольцо защиты
- Накладные расходы



Shadow-Box

- Гипервизорная система защиты для Linux
- Защита памяти
- Защита привилегированных регистров
- Периодические проверки

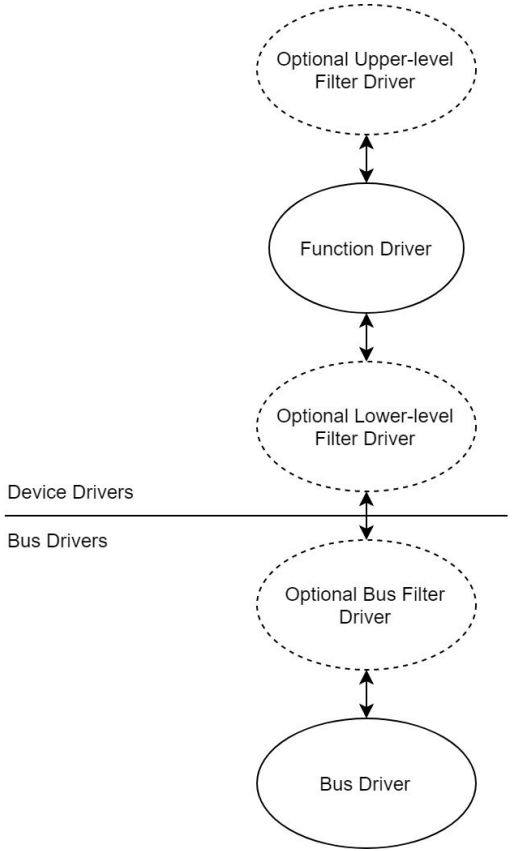


HyperPlatform

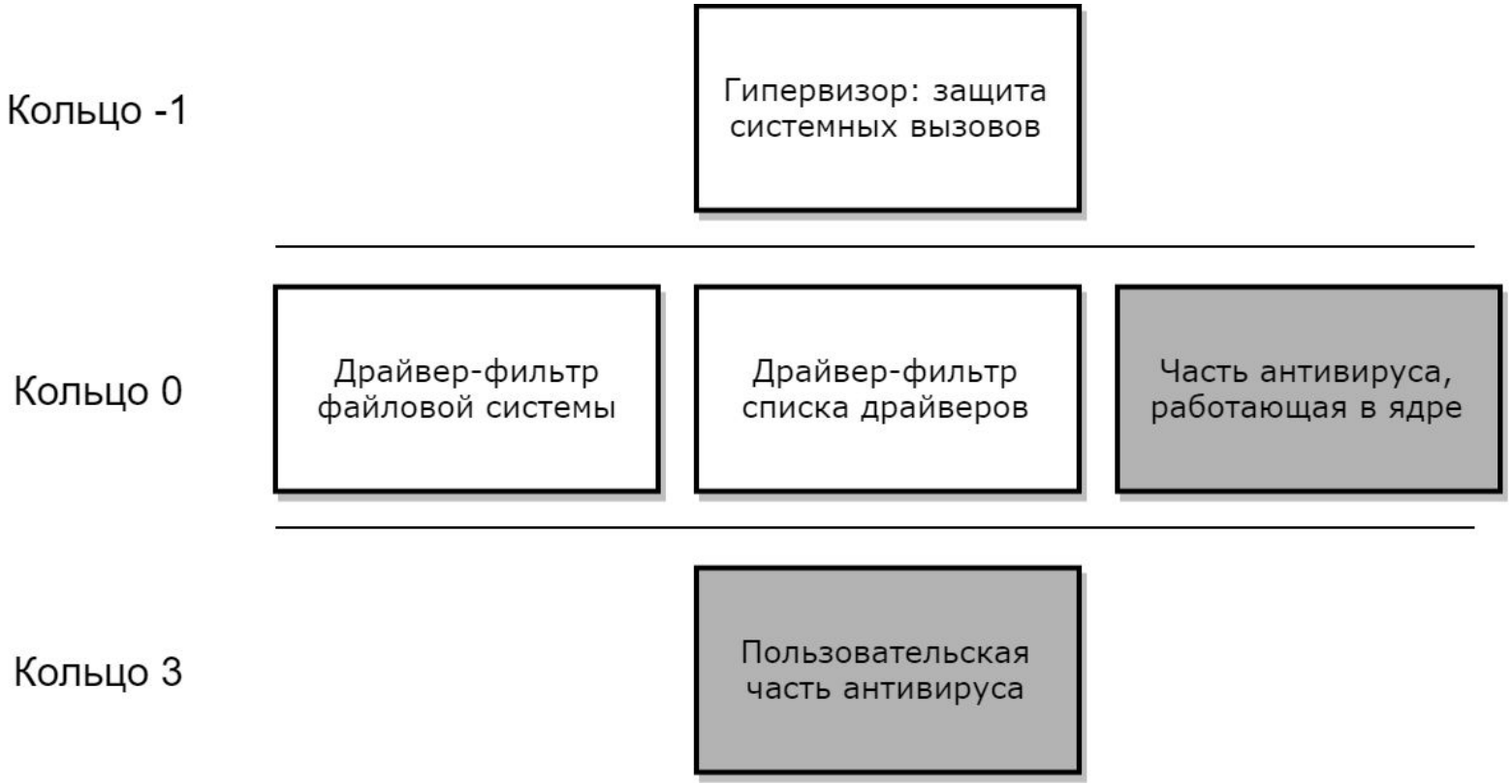
- Гипервизор для Windows
  1. Анализа руткитов
  2. Реверс-инжиниринг ядра ОС
  3. Разработка системы предотвращения вторжений (VIPS)

Windows Driver Frameworks

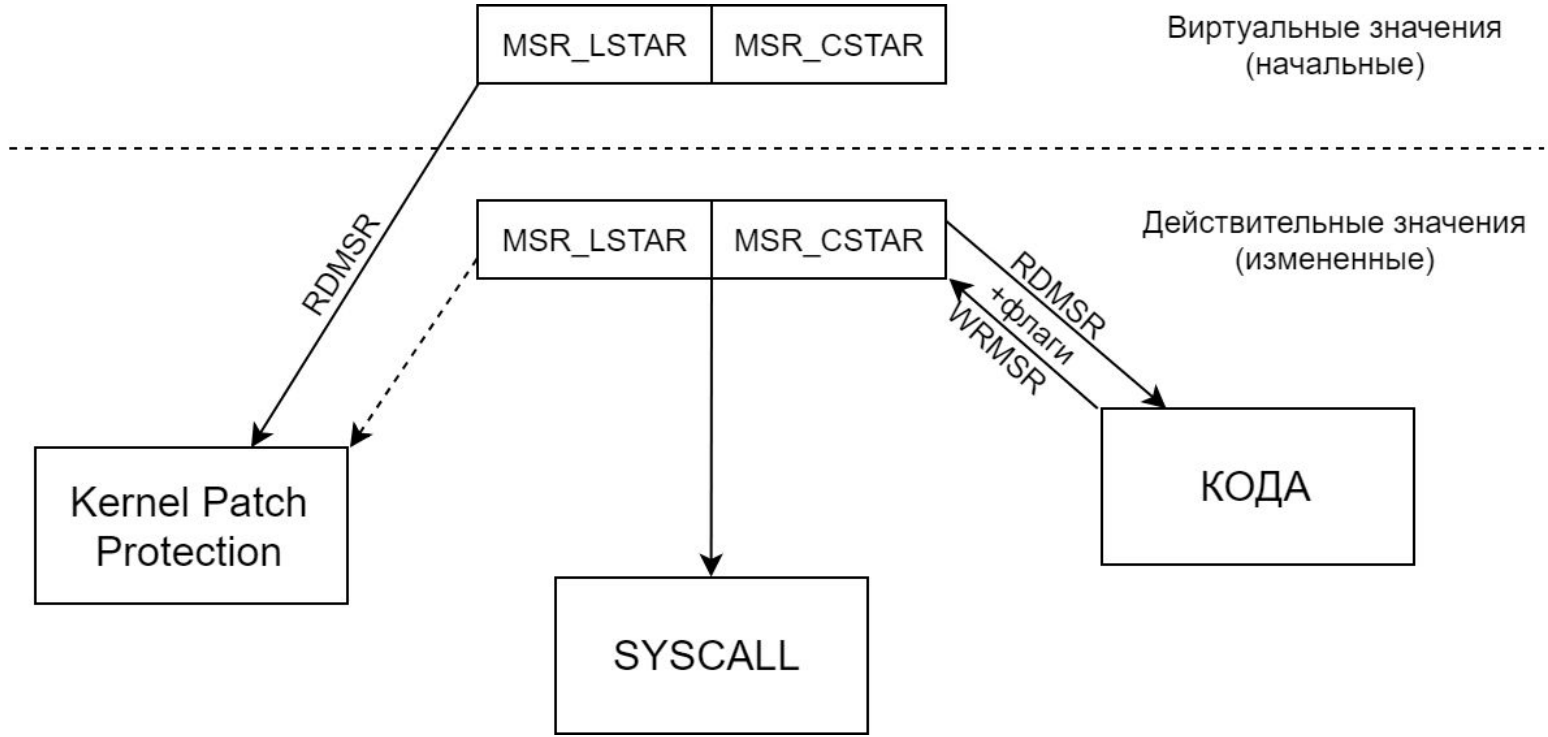
- Драйверы шины
- Драйверы устройств
- Драйверы-фильтры



Архитектура

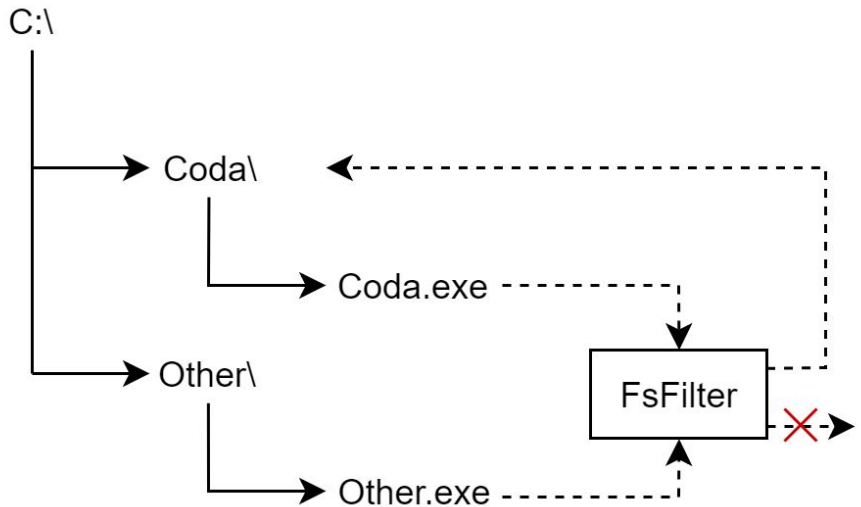


Защита перехватчика системных вызовов



Защита файлов и процессов

- Файловая система
  - Запрет доступа к папкам и файлам
  - Предоставление доступа для программ внутри этих папок
- Список драйверов
  - Direct kernel object manipulation
  - Сокрытие из списка драйверов



Тестирование

- Работа антивируса КОДА
  - Корректное продолжение работы при срабатывании Kernel Patch Protection
- Приложение для файловой системы
  - Попытки обращения к защищенным директориям
- Поиск через NtQuerySystemInformation
  - Перебор списка загруженных модулей

Тестирование производительности

- 10 запусков каждого теста

	Winsat formal: процессор	Winsat formal: жесткий диск	Octane 2.0
Результаты без системы защиты	414±2.67 МБайт/с	105±2.53 МБайт/с	22426±1158
Результаты с системой защиты	403±2.46 МБайт/с	99±2.42 МБайт/с	20873±1051
Избыточная нагрузка	2.59%	5.90%	6,92%

Результаты

- Разработана система защиты антивируса КОДА
  - Перехватчики системных вызовов
  - Файлы на диске
  - Процессы
- Протестирована производительность системы
- Выступление на конференции СПИСОК 2019