Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Технологии защиты от реверс-инжиниринга

Бакаляров Михаил,
Руководитель департамента разработки Guardant

Компания «Актив»

- Технологии безопасности Device Guard в Windows 10
- Протектор кода от RE
- Изменение требований к драйверам Windows для совместимости с Device Guard
- Виртуализация кода, как метод автоматической защиты от копирования в доверенной среде

Протектор кода от RE

Ключевые возможности:

- Виртуализация отдельных функций приложения
  - Накрытие функций целиком
  - Частичное накрытие функций по результатам профайлера
  - Шифрование байт-кода
- Конверт
  - Упаковка и шифрование секций исполняемого файла
  - Защита импортов (.exe, .dll)
- Защита форматов
  - Объектные файлы Windows/Linux (.obj, .o)
  - Исполняемые файлы Windows/Linux (.exe)
  - Драйвера Windows (.sys)
  - Динамические библиотеки Windows/Linux (.dll,.so)
- Кроссплатформенность

Протектор кода от RE

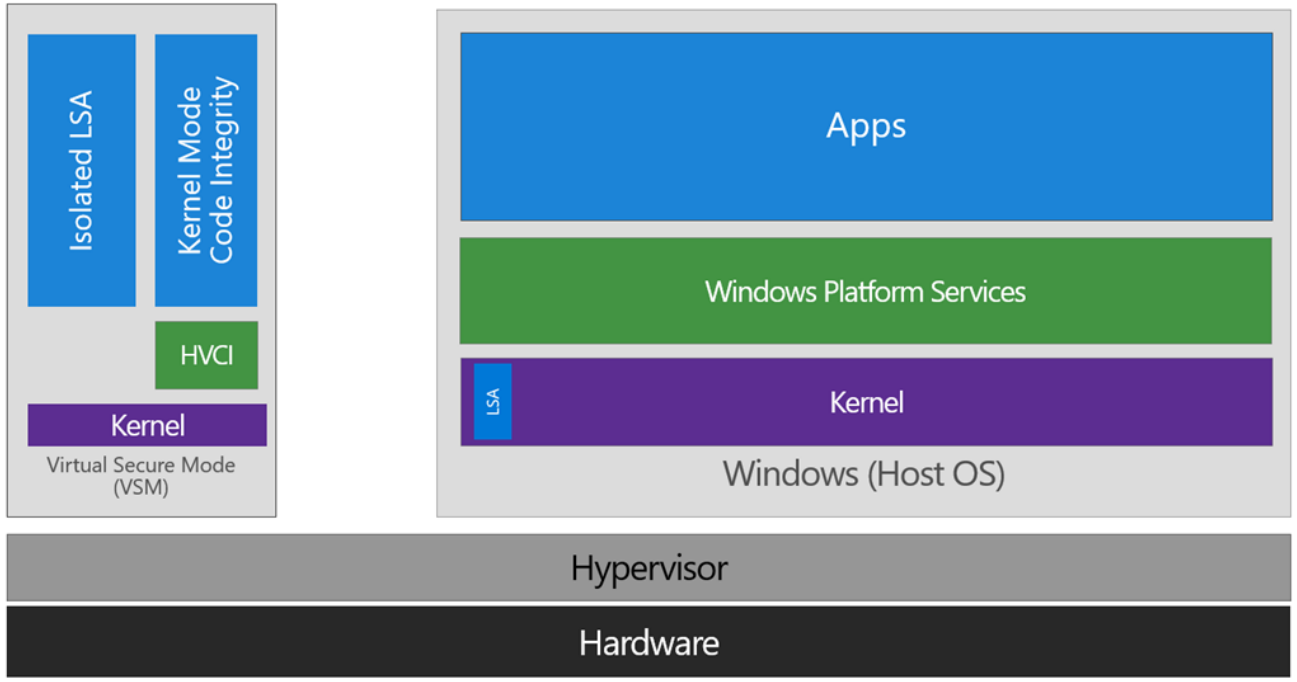
Необходимость поддержки изменений внешней среды:

- Появление новых угроз
- Новые инструкции процессора
- Новые возможности компиляторов
- Повышение безопасности со стороны операционных систем

Device Guard в Microsoft Windows

- Набор технологий безопасности Virtualization-based Security (VBS)
  - **Virtual Secure Mode (VSM)**

Запущен на гипервизоре и отделен от хостовой Window 10 и её ядра.



Device Guard в Microsoft Windows

- Device Guard - Набор компонентов для предотвращения запуска вредоносного кода
  - **Configurable Code Integrity (CCI)**

  Гарантирует, что только доверенный код запускается из загрузчика и далее.
  - **VSM Protected Code Integrity**

  Перемещает компоненты целостности кода режима ядра (KMCI) и целостности кода, контроль за которой осуществляет гипервизор (HVCI) в VSM, защищая их от атак.
  - **Platform and UEFI Secure Boot**

  Позволяет убедиться, что загрузчик (bootloader) и прошивка UEFI подписаны и не были изменены.

Изменение требований к драйверам Windows

- Новые правила игры в Windows Kernel Mode
  - **Требуется цифровая подпись кодовых секций загруженных драйверов и ядра**
  - **Драйверам нельзя иметь секции в sys-файле , которые комбинируют атрибуты защиты W+X (Writable + Executable), либо выравнивание которых меньше размера страницы памяти (4096)**
  - **Запрещена модификация исполняемого кода в любой форме**
  - **Нельзя выполнять некоторые привилегированных инструкций**

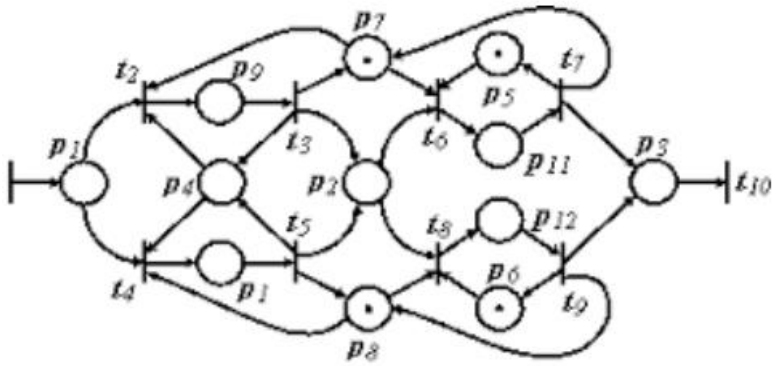
Совместимость с Device Guard

- Доработка защитных механизмов драйверов для совместимости с Device Guard
  - Потребовалось отключение упаковки, т.к. модификация исполняемого кода теперь запрещена в любой форме
  - Нельзя использовать механизмы повторного отображения страниц пользовательского режима на режим ядра с целью передачи туда управления
- Новый метод автоматической защиты в доверенной среде
  - Невозможно выполнить автоматическую защиту от копирования на базе привычной упаковки

Автоматическая защита в доверенной среде

- Виртуализация кода - метод защиты от реверс-инжиниринга

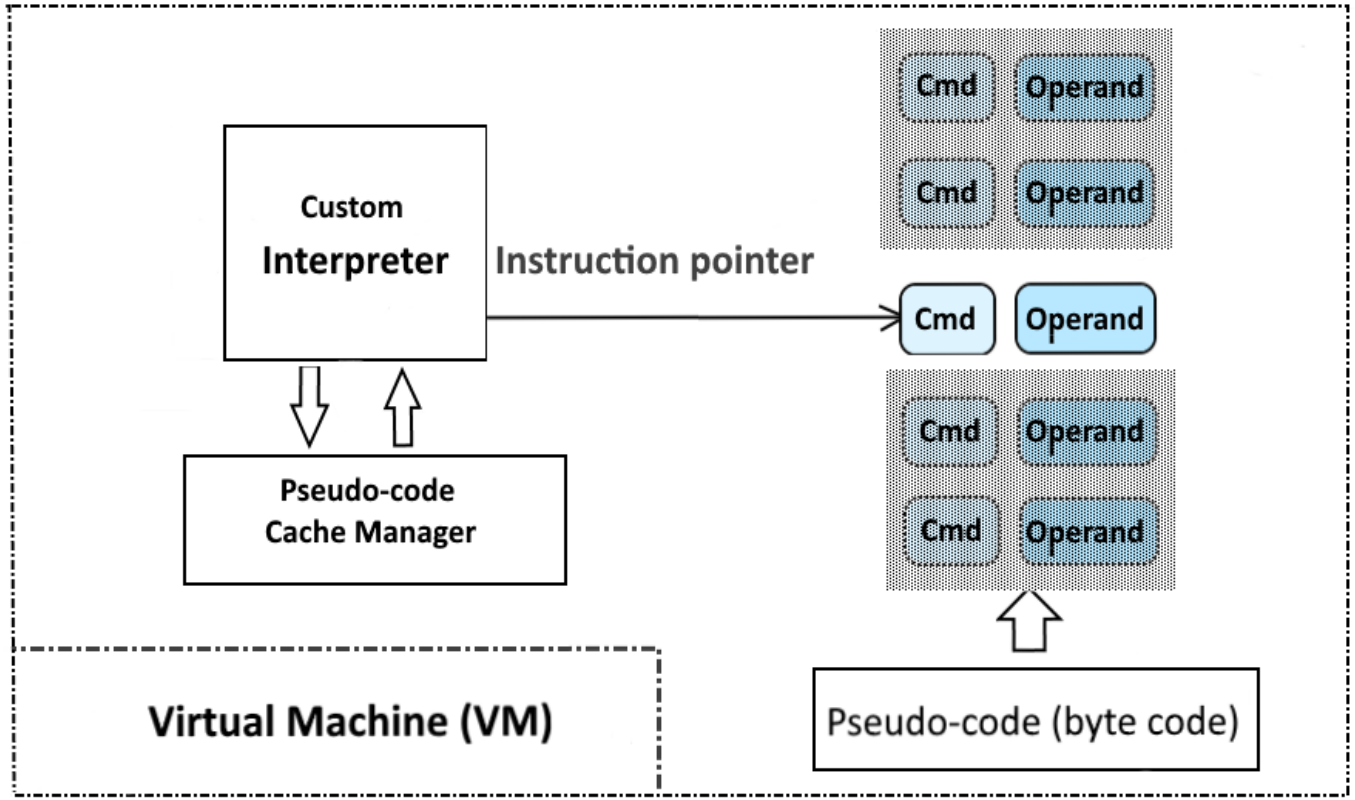
  - **Трансляция кода команды, операндов и флагов в уникальную систему команд и регистров**
  - **Эмуляция флагов процессора**
  - **Использование эквивалентных выражений**
  - **Добавление ложных ветвлений (сети Петри)**
  - **Выражение логических операций через базисы И-НЕ , ИЛИ-НЕ**



$$\overline{x} = x|x = x \downarrow x$$
$$x \vee y = (x|x)|(y|y) = (x \downarrow y) \downarrow (x \downarrow y)$$
$$x \wedge y = (x|y)|(x|y) = (x \downarrow x) \downarrow (y \downarrow y)$$

Автоматическая защита в доверенной среде

- Шифрование байт-кода
  - **Разбиение на блоки**
  - **Защита от дампа**
  - **Лицензирование функций**



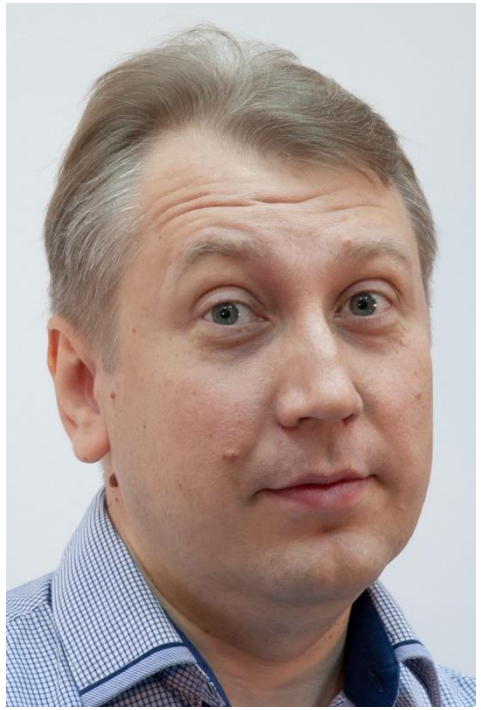
Автоматическая защита в доверенной среде

- Выводы
  - **Упаковка больше не работает**
  - **В доверенной среде актуальной защитой остается виртуализация кода**
  - **Вместо исполняемого кода можно шифровать байт код защищаемых функций**

Вопросы

Контактная информация

Михаил Бакаляров



Электронная почта:

bma@guardant.ru

Телефон:

+7 903 198-23-39

Сайты:

www.guardant.ru

www.aktiv-company.ru