DEFCON RUSSIA

Аппаратная виртуализация и вредоносное ПО

Никита Абдуллин
nabdullin@gmail.com

15.07.2011

Аппаратная виртуализация и вредоносное ПО

- Виртуализация
- Добрые и злые гипервизоры
- Обнаружение гипервизоров и атаки на них
- Противодействие обнаружению
- Перспективы

Аппаратная виртуализация и вредоносное ПО

- **Виртуализация**
- Добрые и злые гипервизоры
- Обнаружение гипервизоров и атаки на них
- Противодействие обнаружению
- Перспективы

Виртуализация

лат. *virtualis – «обладающий силой»*

лат. v*irtus – превосходство, мощь, достоинство, мужественность*

Виртуализация

лат. *virtualis – «обладающий силой»*

лат. v*irtus – превосходство, мощь, достоинство, мужественность*

Виртуализация

- ~ 1650-е г.г.
  - "being something in essence or fact, though not in name“
- ~ 1960-е г.г.
  - Виртуализация – создание *кажущегося* окружения (для <…>)

Виртуализация

- Зачем:
  - Изоляция
  - Эмуляция
  - Управляемость

Виртуализация

- Виртуализация сервисов
- Виртуализация приложений
- Виртуализация ресурсов
- Виртуализация аппаратуры (платформы, hardware virtualization)
  - Полная (QEMU, например)
  - (Частичная)
  - Паравиртуализация (Xen, KVM, …)

Аппаратная виртуализация

Виртуализация аппаратуры
(hardware virtualization)

VS.

Аппаратная виртуализация
(hardware-based virtualization)

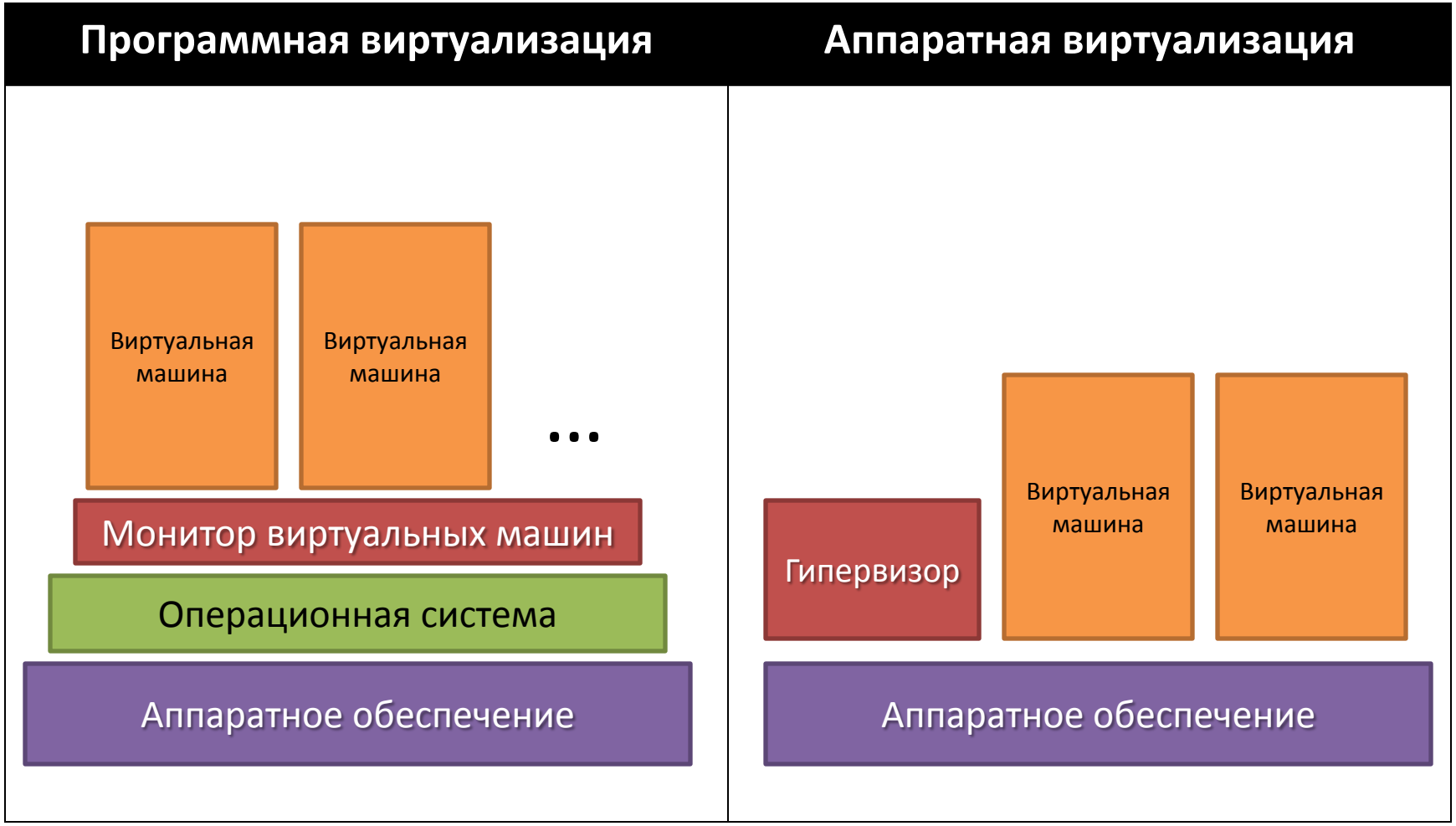
Аппаратная виртуализация

Программная виртуализация
(software-based virtualization)

VS.

Аппаратная виртуализация
(hardware-based virtualization)

Аппаратная виртуализация



Аппаратная виртуализация

- **Аппаратная виртуализация** (hardware-assisted/hardware-based virtualization, HVM, VMX) – семейство технологий, позволяющих предоставлять для программной среды (ОС) полностью эмулируемое (виртуальное) окружение с прозрачным доступом к аппаратному обеспечению.

Аппаратная виртуализация

- 1964 – IBM CP/40 – полная
- 1966 – IBM M44/44X – пара + вирт.память
- 1972 – IBM VM/370 – гипервизор
- 1974 – критерии Попека-Голдберга
- 1998 – VMWare
- 2005 – Intel, AMD – расширения для аппаратной виртуализации

Критерии Попека-Голдберга

- Принципы
  - Эквивалентность
  - Эффективность
  - Контроль VMM над ресурсами
- Набор инструкций
  - Привилегированные
  - Чувствительные по управлению
  - Чувствительные по поведению
- Требования
  1. $чувствительные \subseteq привилегированные$
  2. если нет задержек → вложенная виртуализация

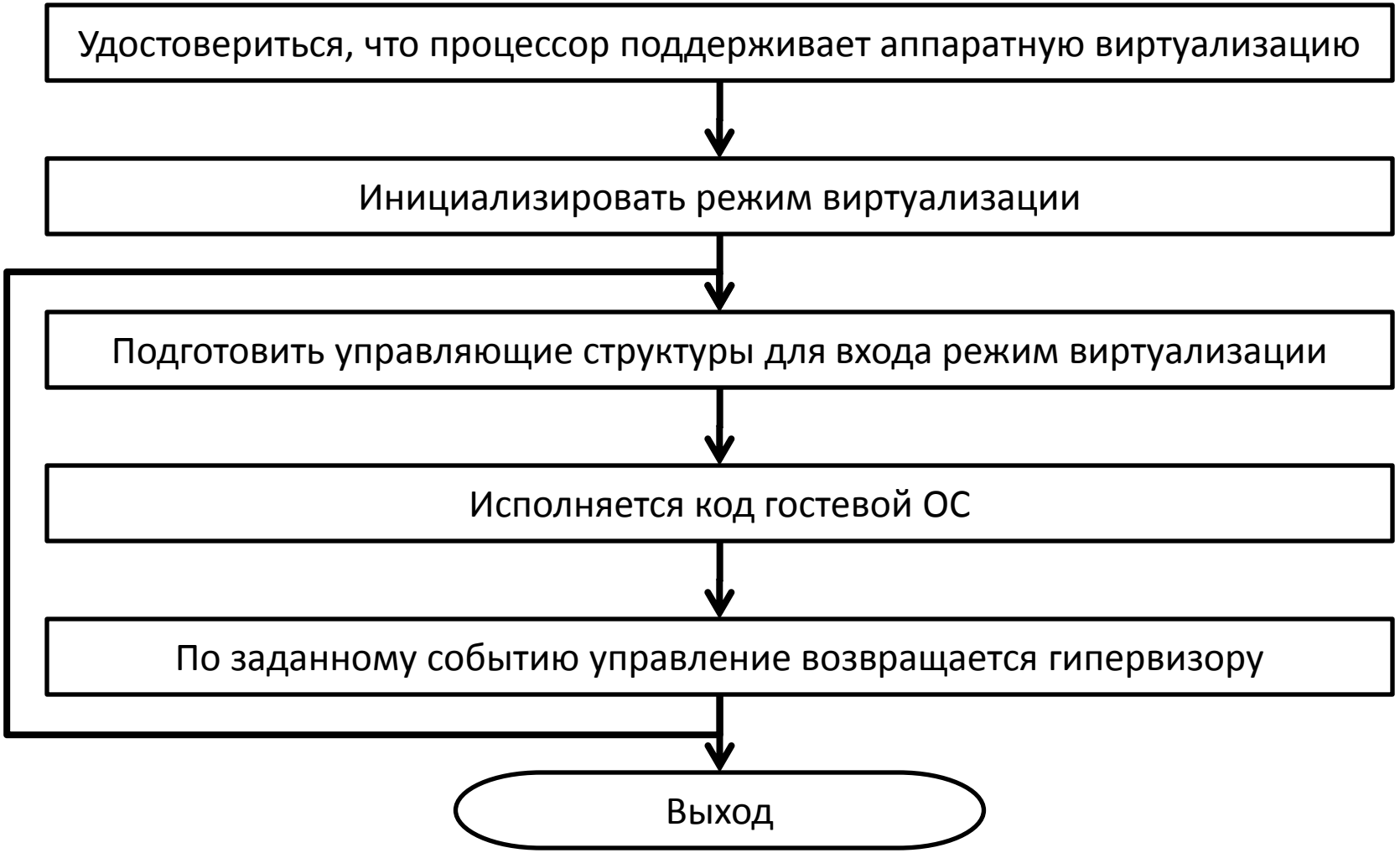
Аппаратная виртуализация

- Intel VT, AMD-V
- Управление непосредственным доступом из виртуальной среды к реальным устройствам
  - AMD IOMMU
  - Intel VT-d
- Поддержка вложенной (nested) виртуализации
  - Intel EPT
  - AMD RVI
- Прочие плюшки

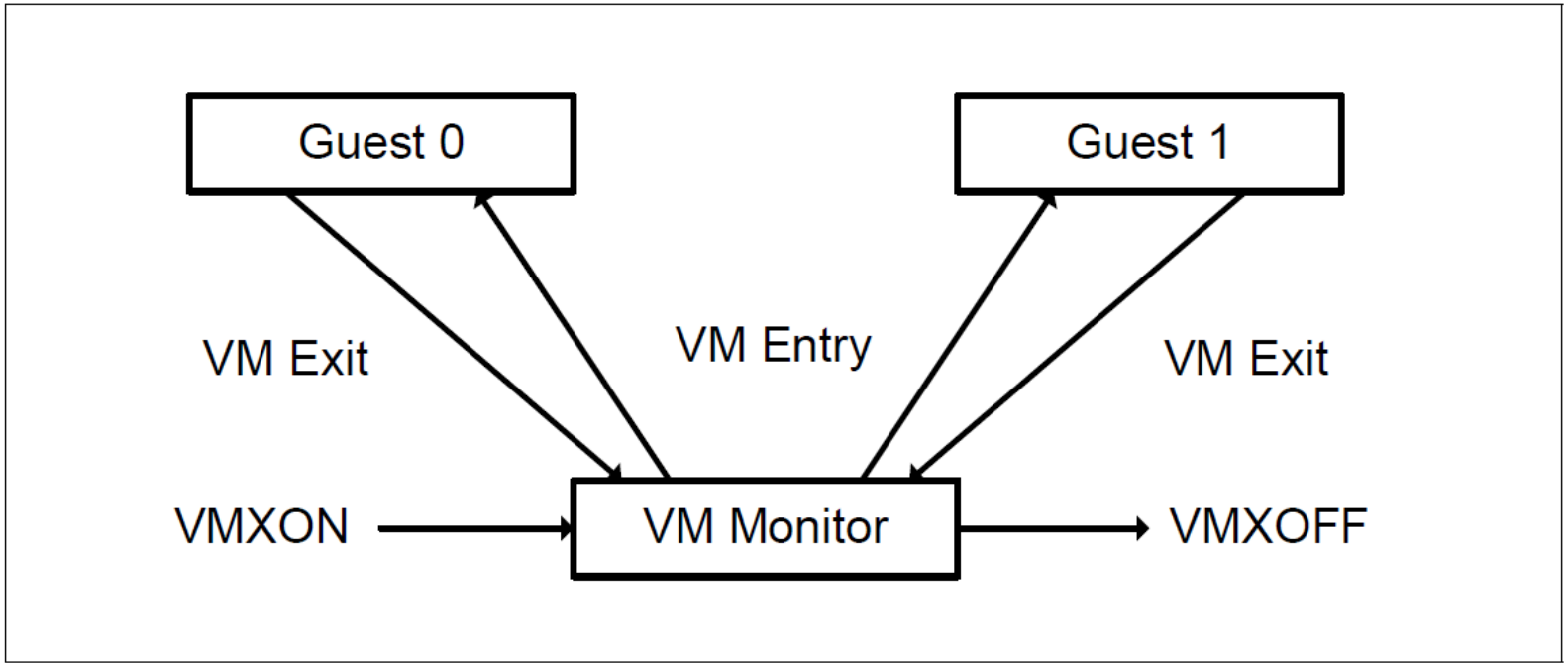
Гипервизор

- Он же VMM (Virtual Machine Monitor)
  - Контролирует гостевые среды
  - Следит за распределением ресурсов
  - Переключает контекст исполнения
  - …

Гипервизор


Удостовериться, что процессор поддерживает аппаратную виртуализацию
Инициализировать режим виртуализации
Подготовить управляющие структуры для входа режим виртуализации
Исполняется код гостевой ОС
По заданному событию управление возвращается гипервизору
Выход

Гипервизор


Guest 0
Guest 1
VM Exit
VM Entry
VM Exit
VMXON
VM Monitor
VMXOFF

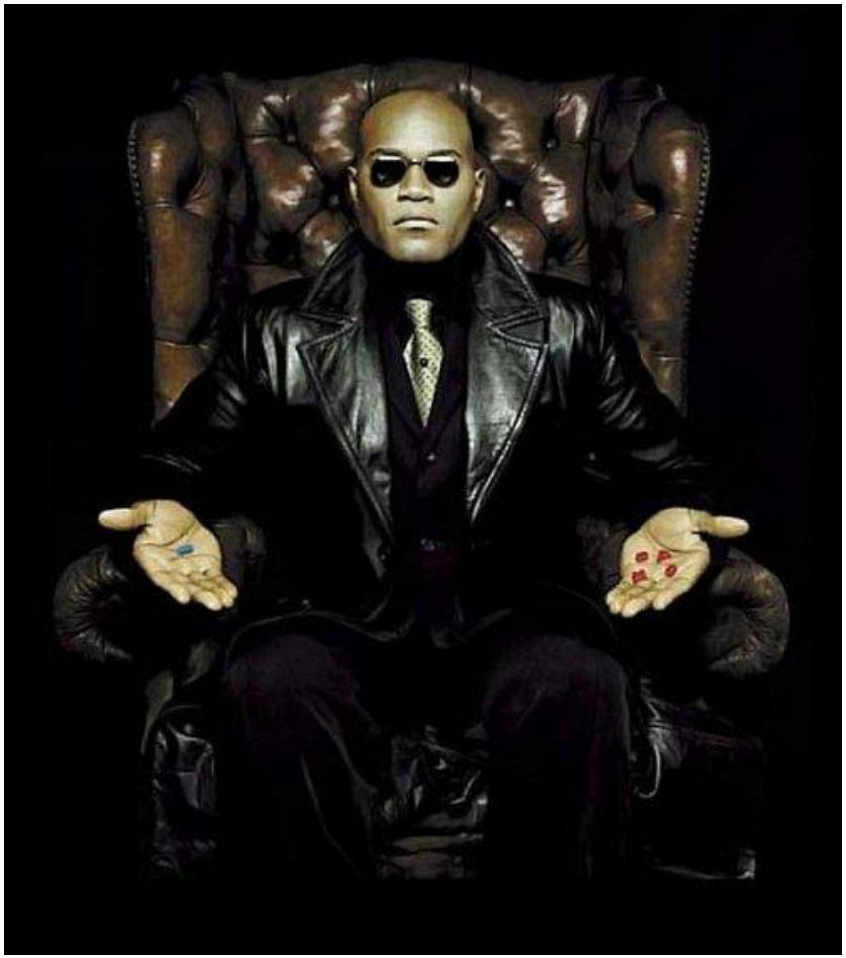
Гипервизор

- Надо управлять исполнением
  - Установка перехватчиков на некоторые инструкции (есть обязательные)
- Надо управлять памятью
  - Структуры управления вирт. памятью
    - Надо поддерживать копии таблицы страниц
      - Shadow page tables/ Nested page tables
  - Что будет в TLB?
    - Будем тегировать записи в TLB

Аппаратная виртуализация и вредоносное ПО

- Виртуализация
- **Добрые и злые гипервизоры**
- Обнаружение гипервизоров и атаки на них
- Противодействие обнаружению
- Перспективы

Добрые гипервизоры



Добрые гипервизоры

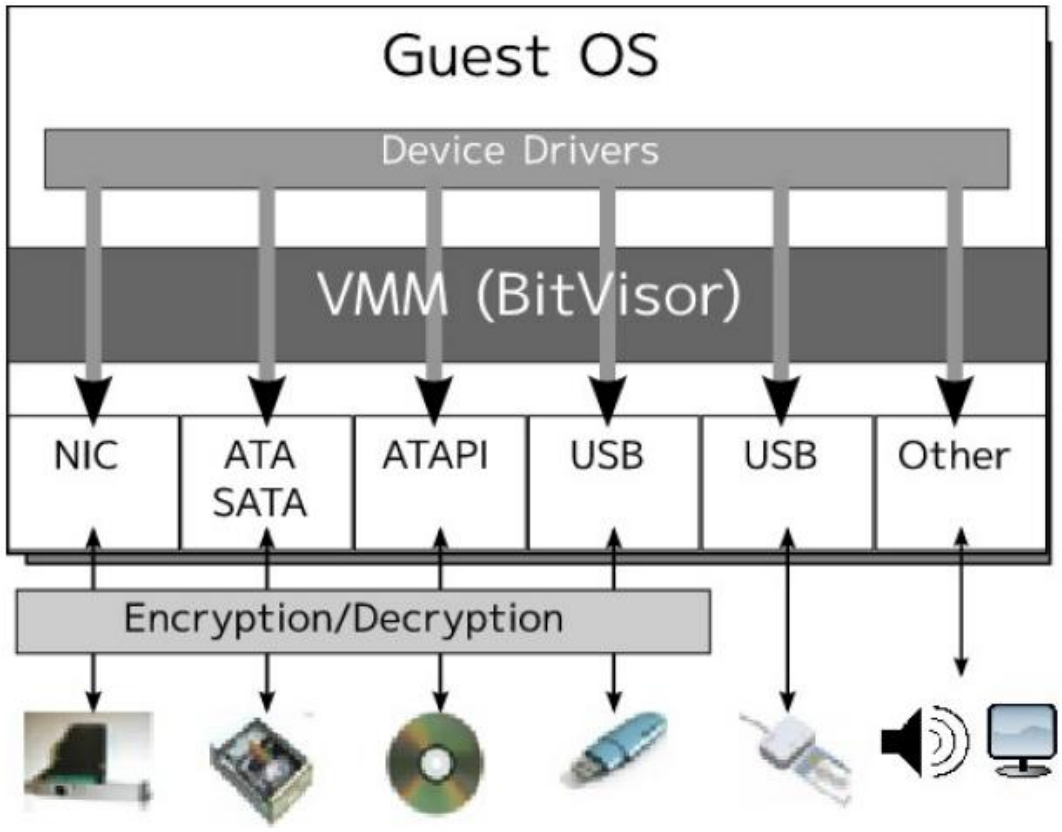
- Гипервизор имеет максимум (?!) полномочий
- Гипервизор может разделять и властвовать
  - А гостевые среды без модификации работают с реальным железом, и почти без накладных расходов

Добрые гипервизоры

- VMM:
  - VMWare
  - MS Virtual PC
  - MS Hyper-V
  - Xen
    - Oracle VM
    - Qubes
  - KVM
  - …

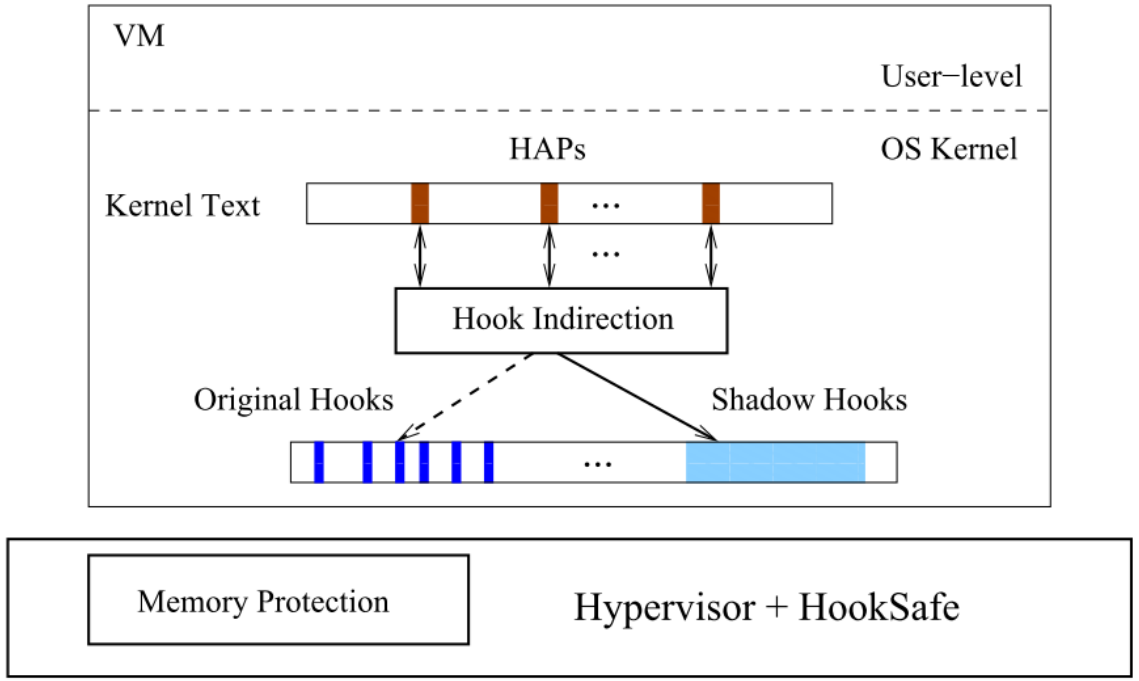
Добрые гипервизоры

- Средства защиты
  - BitVisor
    - Viton



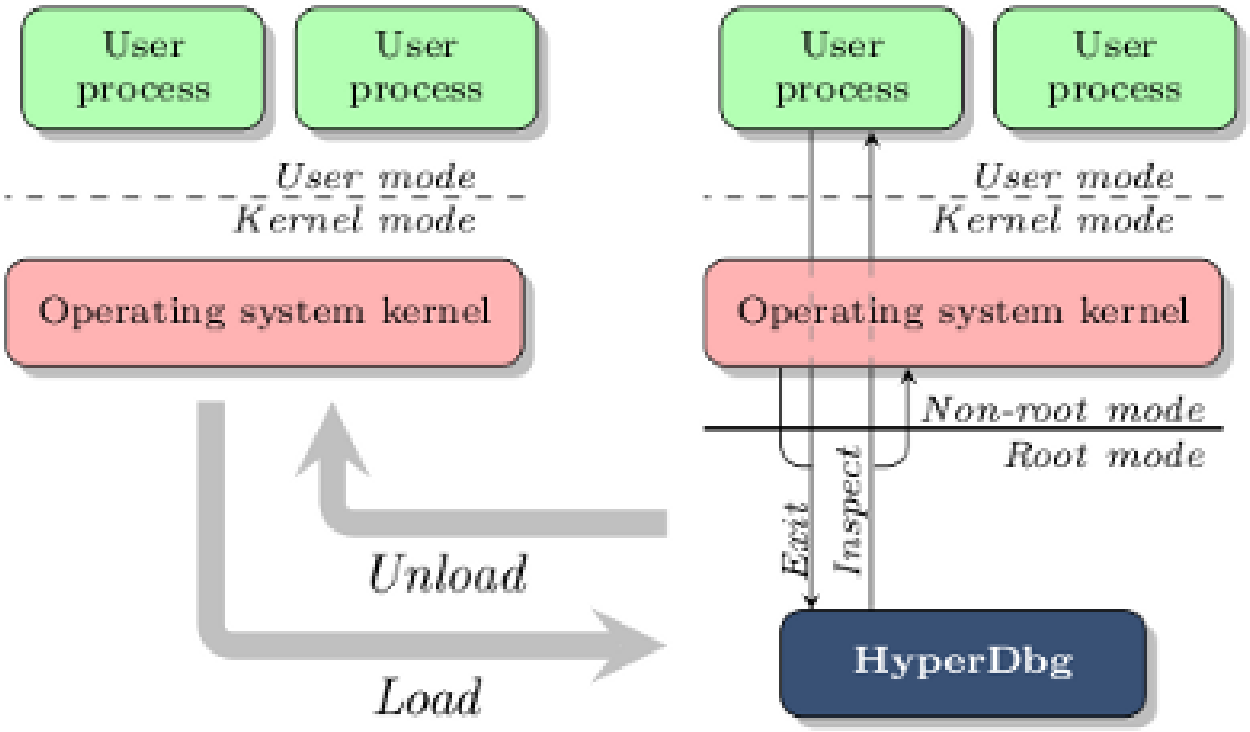
Добрые гипервизоры

- Средства защиты
  - HookSafe
  - HyperSight



Добрые гипервизоры

- Отладчики
  - hyperdbg
  - virtdbg

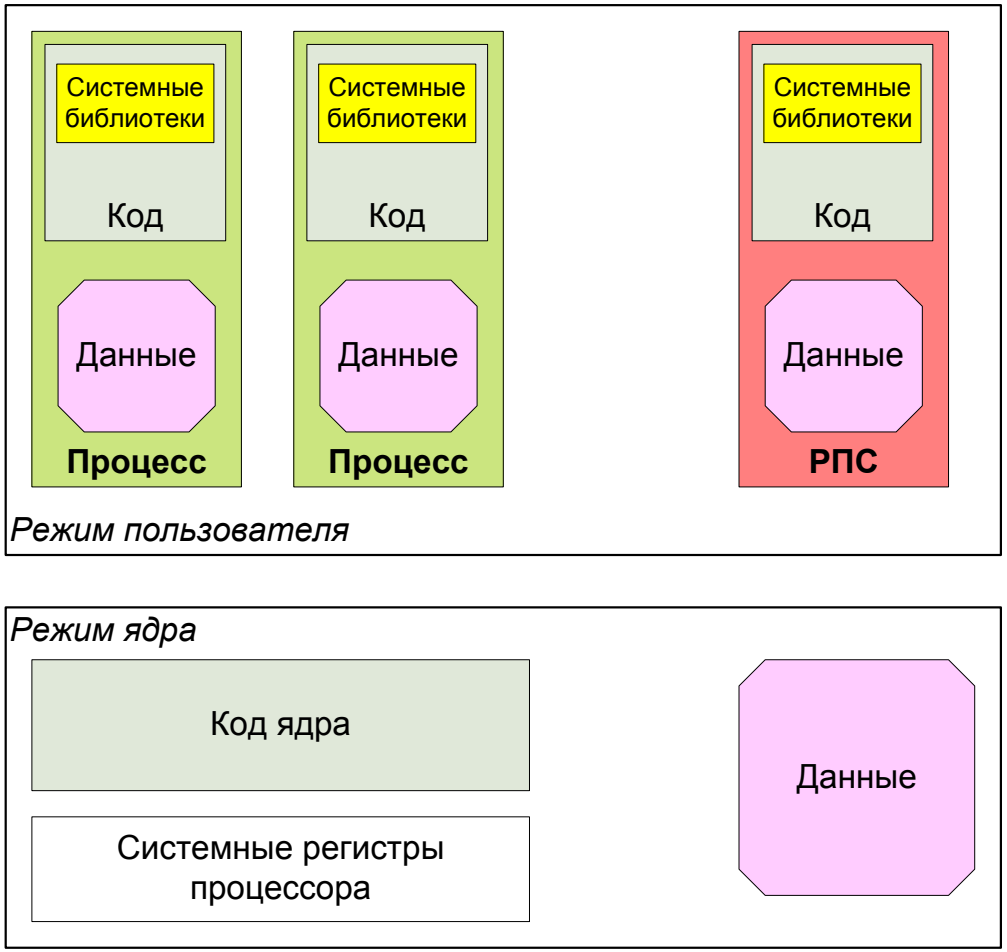


Злые гипервизоры

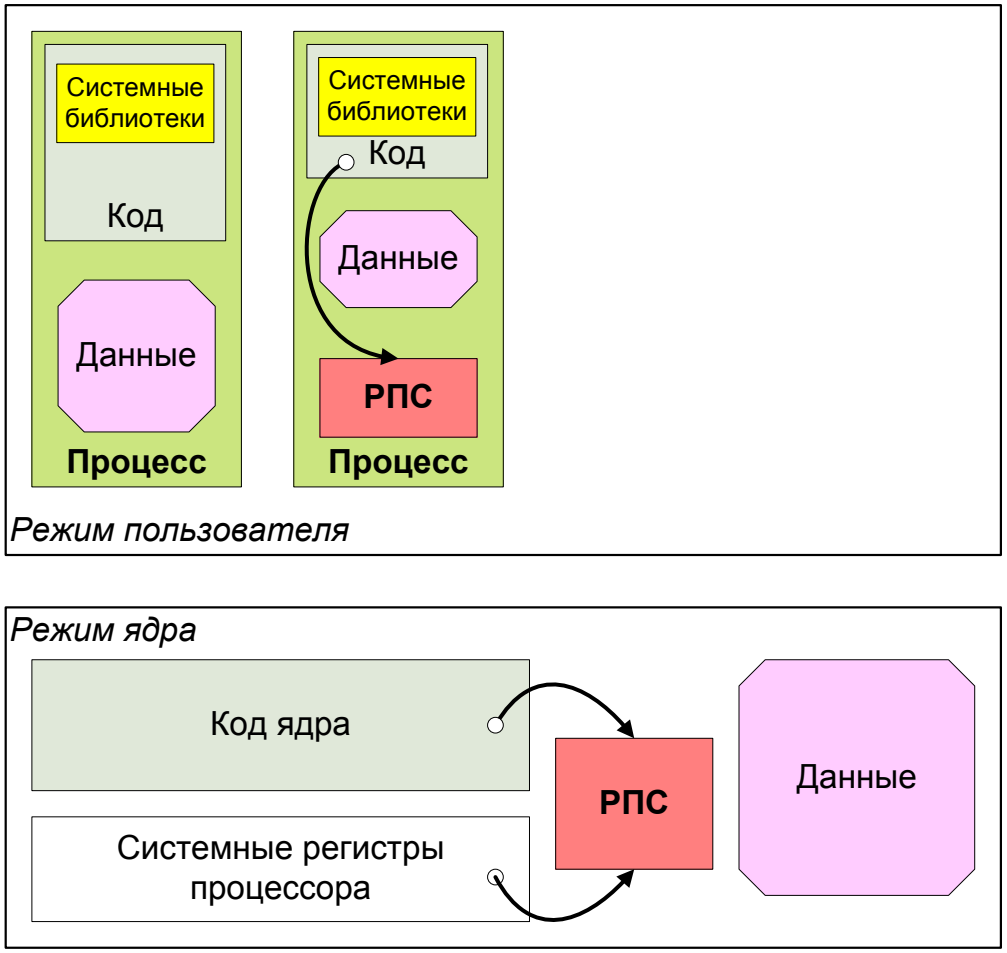
Злые гипервизоры

- 2006, Дж. Рутковска: Introducing Stealth Malware Taxonomy
- 4 типа РПС
  - Тип 0
  - Тип 1
  - Тип 2
  - Тип 3

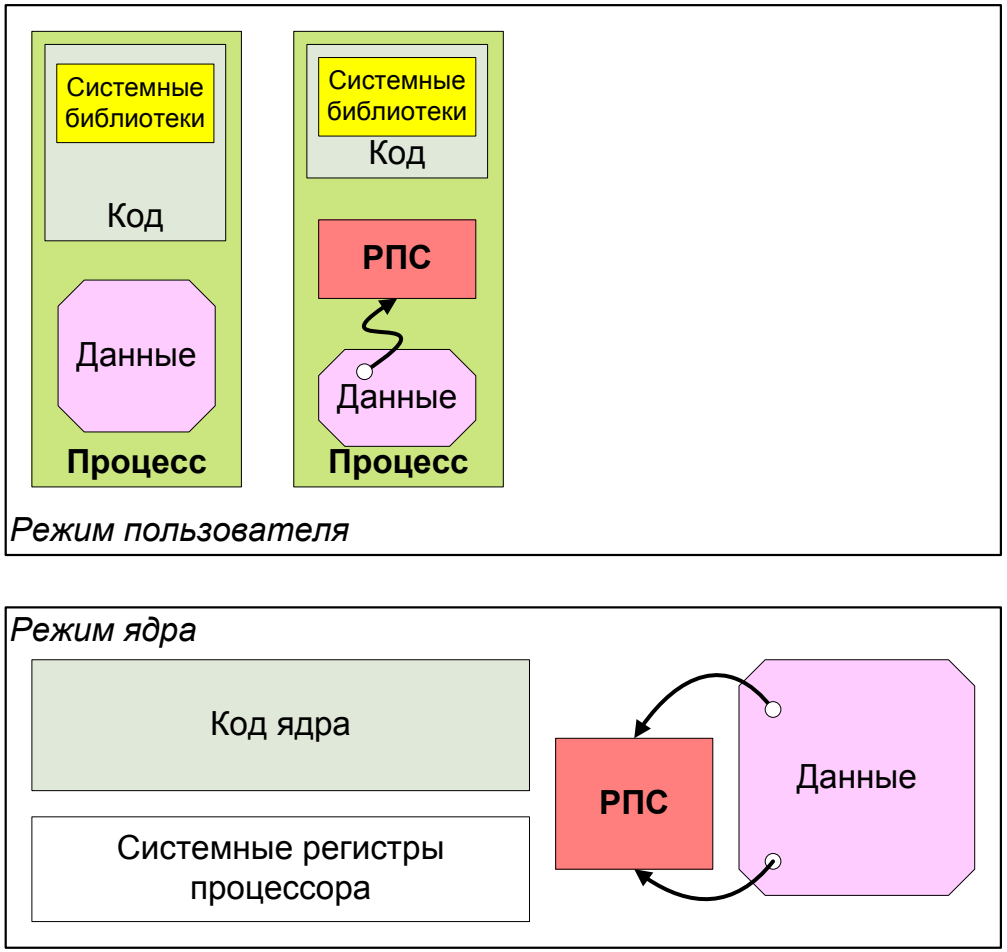
РПС типа 0


Системные библиотеки
Код
Данные
Процесс
Системные библиотеки
Код
Данные
Процесс
Системные библиотеки
Код
Данные
РПС
Режим пользователя
Режим ядра
Код ядра
Системные регистры процессора
Данные

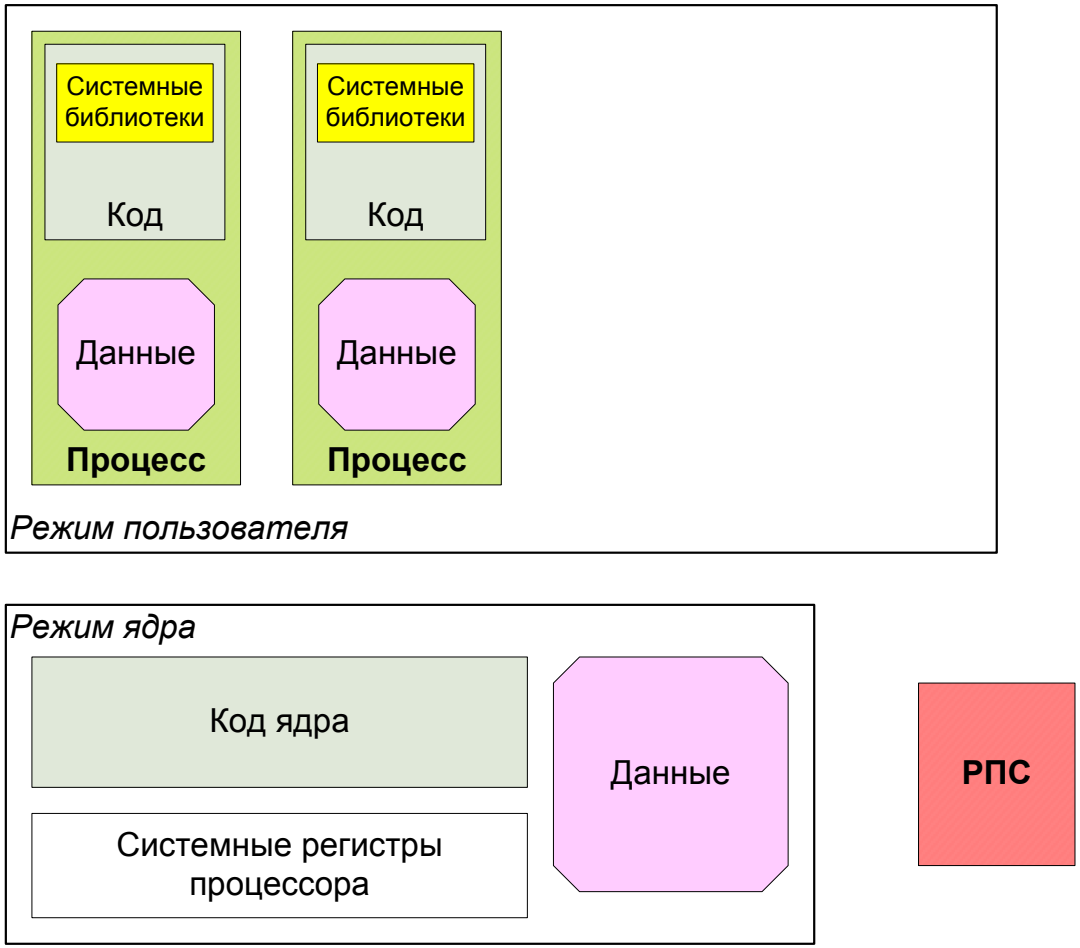
РПС типа 1


Системные библиотеки
Код
Данные
Процесс
Системные библиотеки
Код
Данные
РПС
Процесс
Режим пользователя
Режим ядра
Код ядра
Системные регистры процессора
РПС
Данные

РПС типа 2


Системные библиотеки
Код
Данные
Процесс
Системные библиотеки
Код
РПС
Данные
Процесс
Режим пользователя
Режим ядра
Код ядра
Системные регистры процессора
РПС
Данные

РПС типа 3


Системные библиотеки
Код
Данные
Процесс
Системные библиотеки
Код
Данные
Процесс
Режим пользователя
Режим ядра
Код ядра
Системные регистры процессора
Данные
РПС

РПС типа 3

- SMM (System Maintenance Mode)
  - Наиболее привилегированный режим процессора, предназначенный для узкоспециализированных задач настройки и диагностики
- Специфические уязвимости в аппаратном обеспечении
  - 2008, Ю.Булыгин
  - 2008, А.Терешкин, R. Wojtczuk: РПС в чипсете мат. платы
  - 2010, L. Duflot: РПС в сетевом адаптере, внедрение через переполнение аппаратного буфера
- **Аппаратная виртуализация – РПС-гипервизор**

Злые гипервизоры

- Реальных РПС in the wild – не слышно.
- Исследователями созданы:
  1. 2006, MS Research: SubVirt (Windows, Intel VT)
  2. 2006, Dino Dai Zovi: Vitriol (Mac OS X, Intel VT)
  3. 2006-2008, Дж.Рутковска, А.Терешкин: BluePill (Windows, AMD-V и Intel VT)

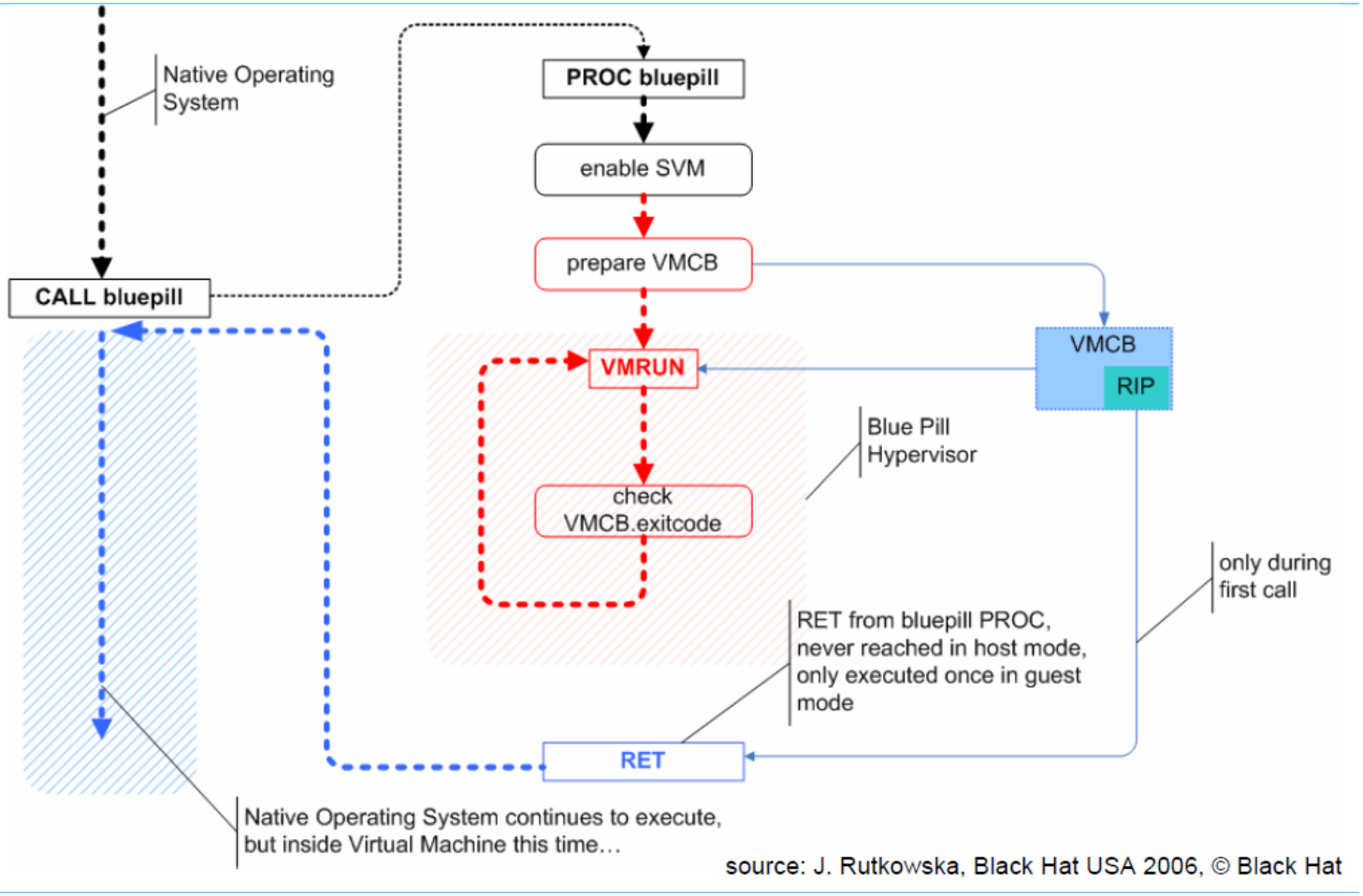
Злые гипервизоры

- Реальных РПС in the wild – не слышно.
- Исследователями созданы:
  1. 2006, MS Research: SubVirt (Windows, Intel VT)
  2. 2006, Dino Dai Zovi: Vitriol (Mac OS X, Intel VT)
  3. 2006-2008, Дж.Рутковска, А.Терешкин: BluePill (Windows, AMD-V и Intel VT)

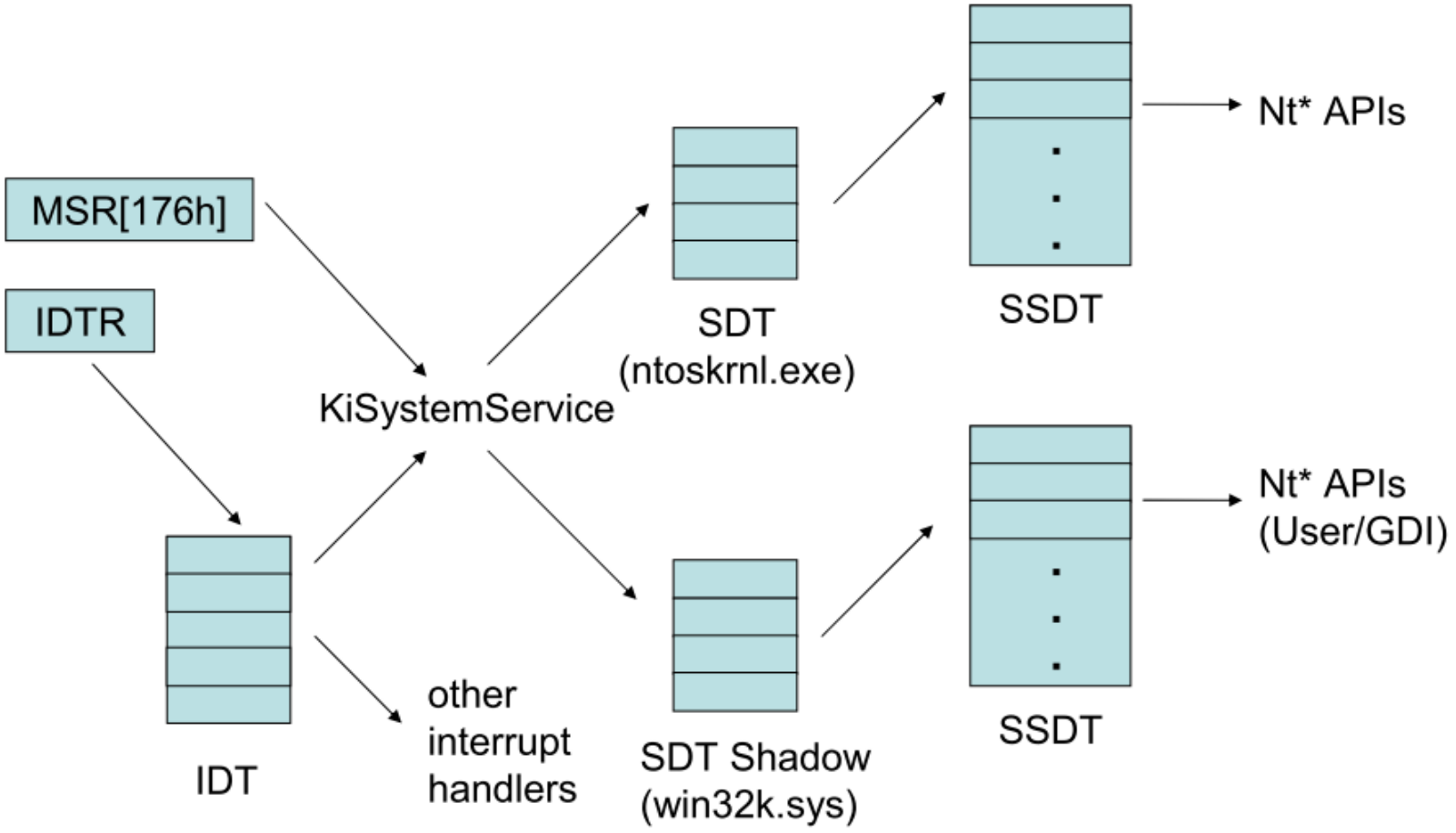
Bluepill

- Изначально – только поддержка AMD-V
- 2007-2008: доступен исходный код модифицированной версии 0.32, поддерживающей Intel VT
- Выполнен в виде драйвера
- Переводит ОС в гостевой режим во время ее работы и почти ничего не делает

Bluepill


Native Operating System
PROC bluepill
enable SVM
prepare VMCB
CALL bluepill
VMRUN
VMCB
RIP
Blue Pill Hypervisor
check VMCB.exitcode
only during first call
RET from bluepill PROC, never reached in host mode, only executed once in guest mode
RET
Native Operating System continues to execute, but inside Virtual Machine this time…
source: J. Rutkowska, Black Hat USA 2006, © Black Hat

Злые гипервизоры



Злые гипервизоры

- И как обнаружить подобное чудо?
  - Гостевая ОС не может выйти за пределы навязанной ей gPT
  - Гипервизор может перехватить любые инструкции и сделать что угодно

Злые гипервизоры

- И как обнаружить подобное чудо?
  - Гостевая ОС не может выйти за пределы навязанной ей gPT
  - Гипервизор может перехватить любые инструкции и сделать что угодно

Аппаратная виртуализация и вредоносное ПО

- Виртуализация
- Добрые и злые гипервизоры
- **Обнаружение гипервизоров и атаки на них**
- Противодействие обнаружению
- Перспективы

Обнаружение гипервизоров

- попытка обнаружить = атака

Обнаружение гипервизоров

- Аппаратная виртуализация не идеальна
  - Накладные расходы
  - CPU bugs
  - Неполный контроль над оборудованием
  - Уязвимости ~~во все поля~~

Атаки, использующие неотъемлемые свойства аппаратной виртуализации

- Атаки на запрещенные в определенных режимах инструкции
  - малая известность - относительно редко используются разработчиками традиционных РПС
  - детерминизм – данная конкретная аппаратная конфигурация содержит фиксированный набор особенностей и ошибок реализации
- Атаки с использованием вложенной виртуализации

Атаки с использованием оценок производительности

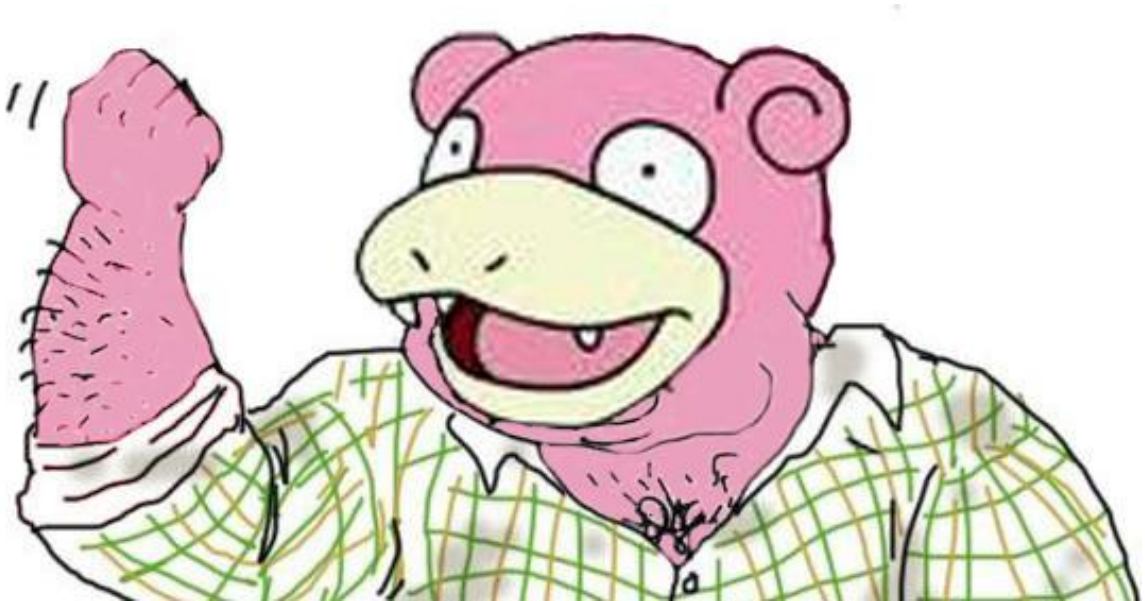
- Атаки с использованием таймеров
  - Базовая оценка производительности с попыткой «поймать» код гипервизора на перехвате
- Атаки с использованием профилирования ресурсов
  - Попытка определить характер использования RAM и кэшей процессора гипервизором
- Атаки с использованием синхронизации
  - Использование нескольких потоков исполнения (ядер) для десинхронизации действий гипервизора на них

Атаки с использованием оценок производительности

- Таймеры – масса вариантов
  - NTP
  - Часы в периферии
  - DSP звуковой карты
  - GPU

Атаки с использованием оценок производительности

- Таймеры – масса вариантов
  - NTP
  - Часы и таймеры в периферии
  - DSP звуковой карты
  - GPU



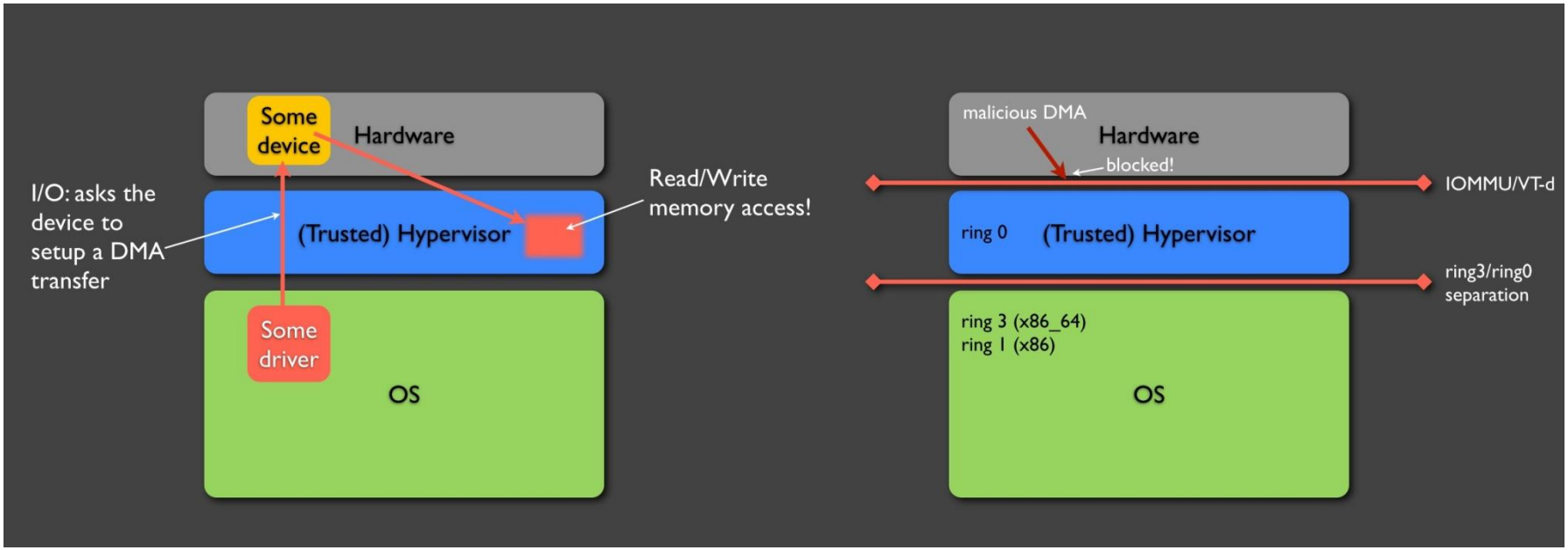
Атаки на конкретные уязвимости

- Дж. Рутковска, А. Терешкин, R.Wojtczuk
  - 2008: Xen owning trilogy
  - 2011: Атака на VT-d в Xen

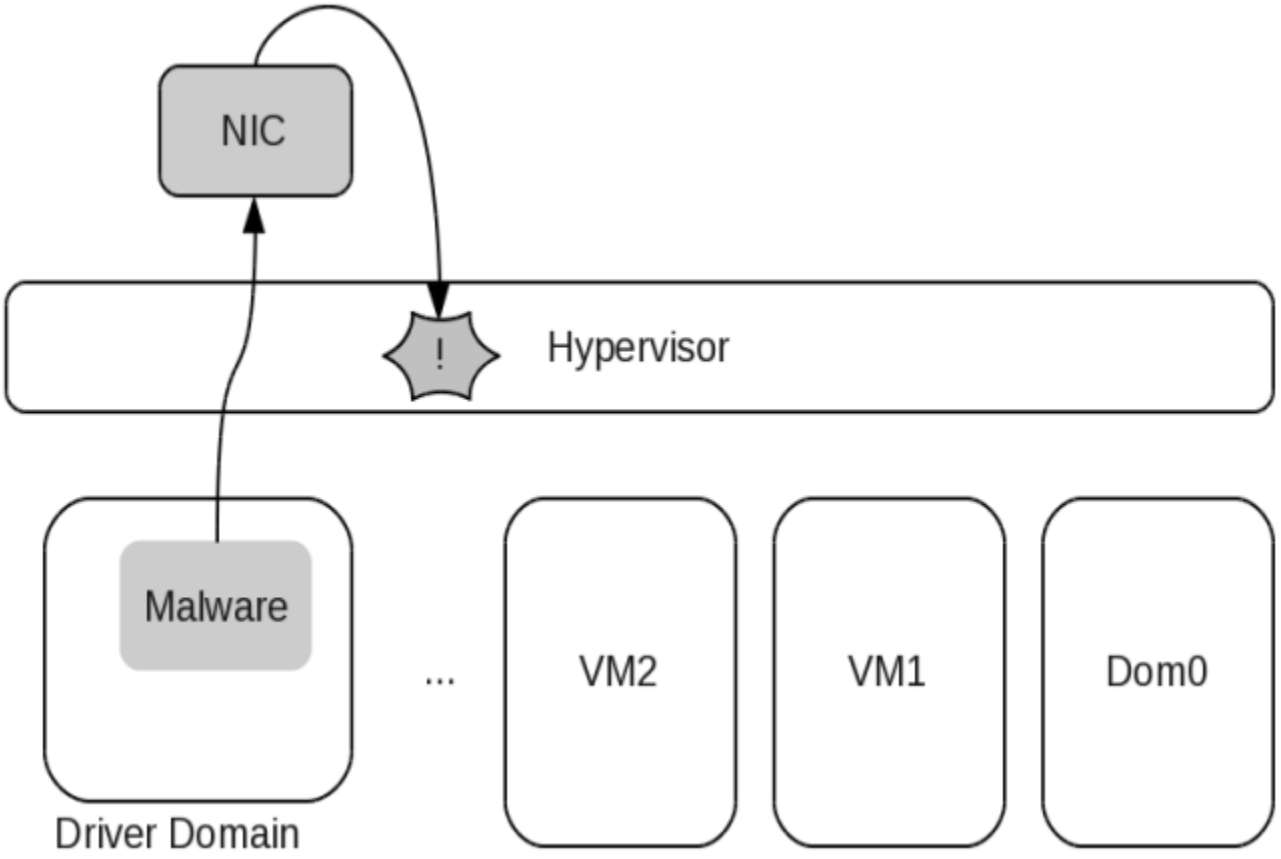
Xen owning trilogy

- Атака на DMA из dom0
  - Драйвера диска и сетевого интерфейса
- Обход VT-d
  - DMA Remapping
  - Баг в конкретном BIOS
- Xen под Bluepill

Xen owning trilogy



Атака на VT-d в Xen



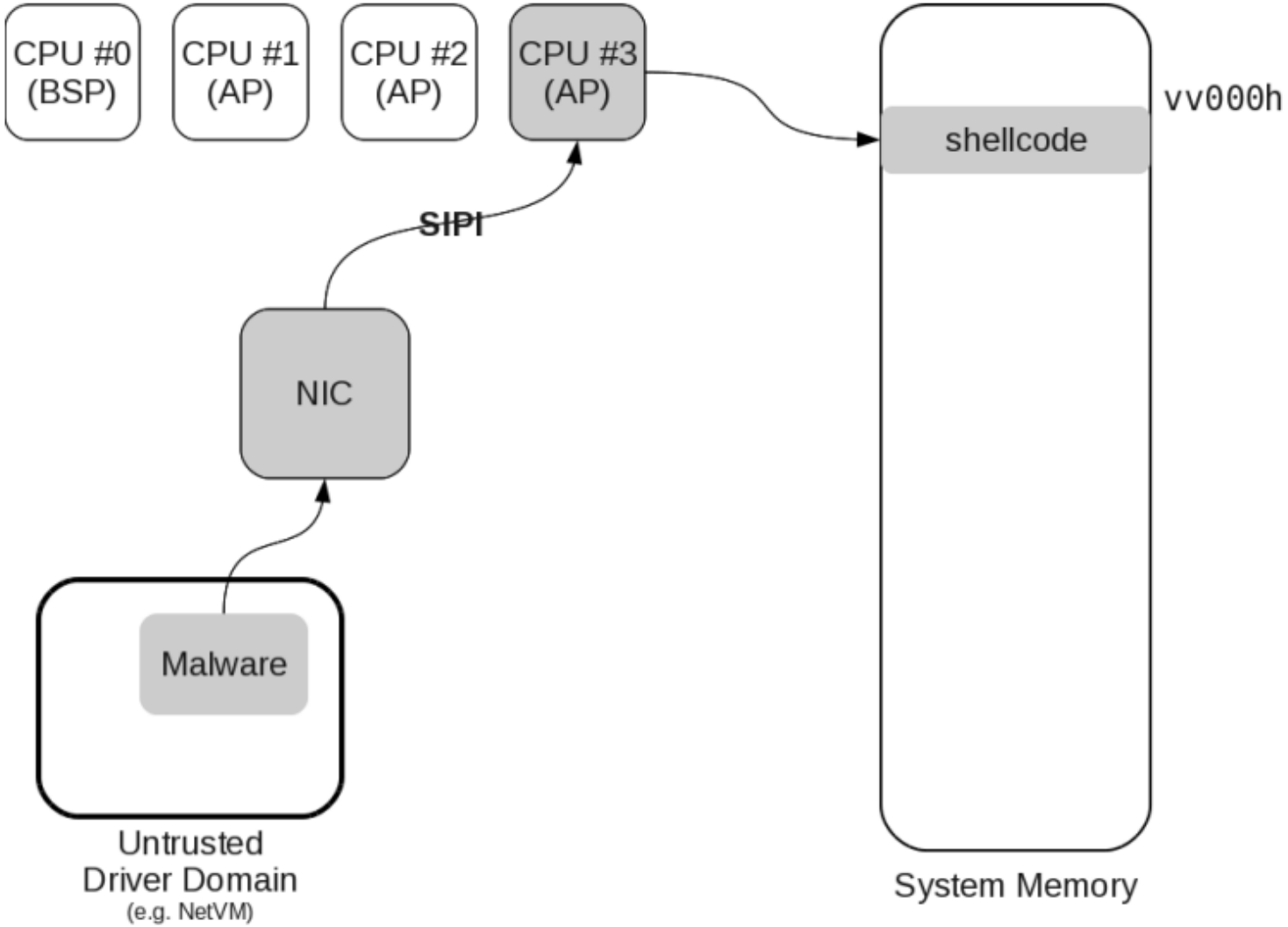
Атака на VT-d в Xen

- MSI (Message Signaling Interrupts)
  - PCI-e транзакция на адрес 0xFEEXXXXX служит определенным сигналом для процессора
  - В пакете MSI передается вектор прерывания (аналогичный тем, что в IDT)
- MSI настраиваются из гостевых доменов
- Генерим MSI особого вида, указывающий куда надо

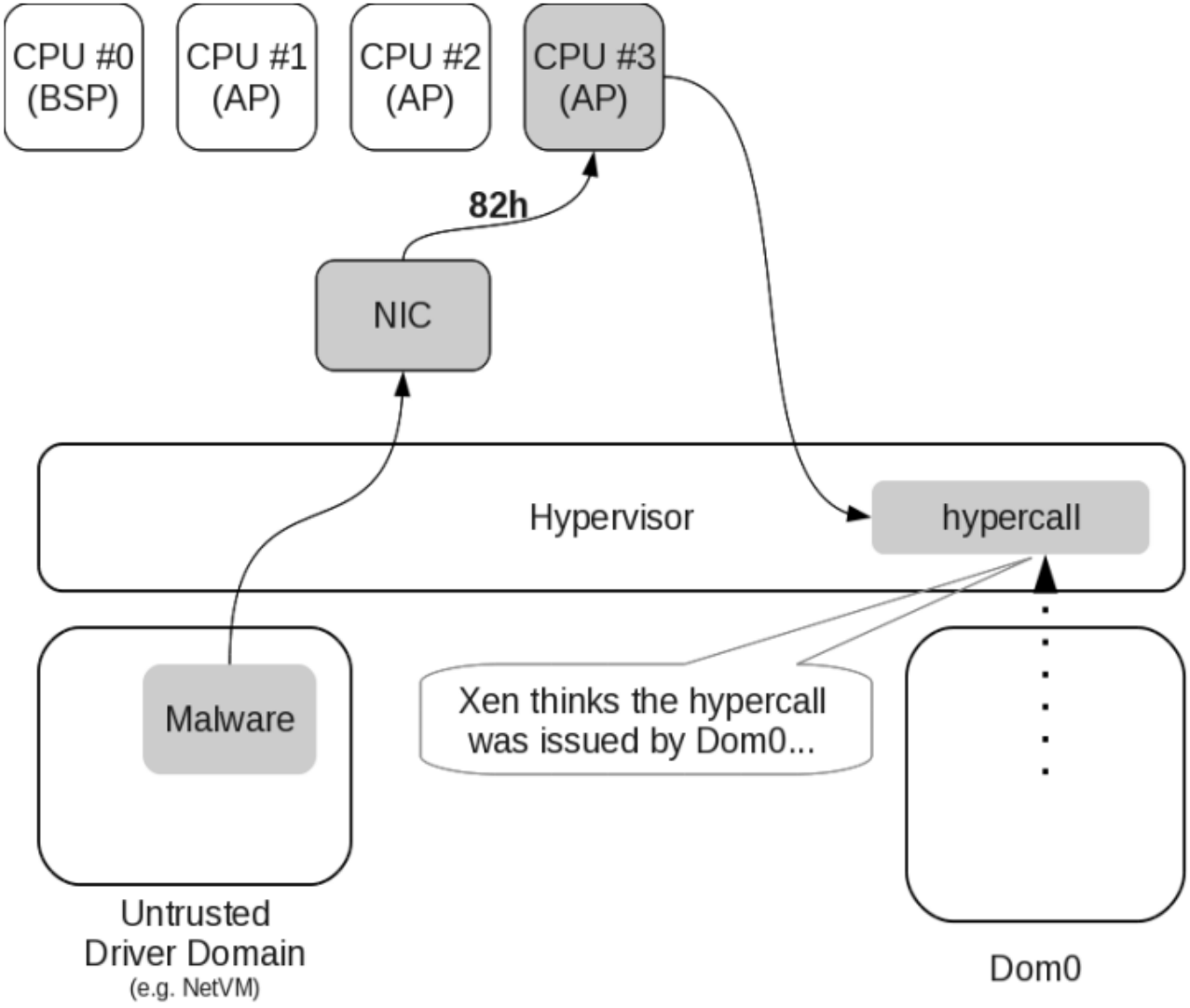
Атака на VT-d в Xen

- SIPI (Start-up Inter Processor Interrupt)
  - BIOS инициализирует многопроцессорную систему используя SIPI
  - SIPI и MSI не просто так похожи
- Инъекция syscall
- Инъекция #AC

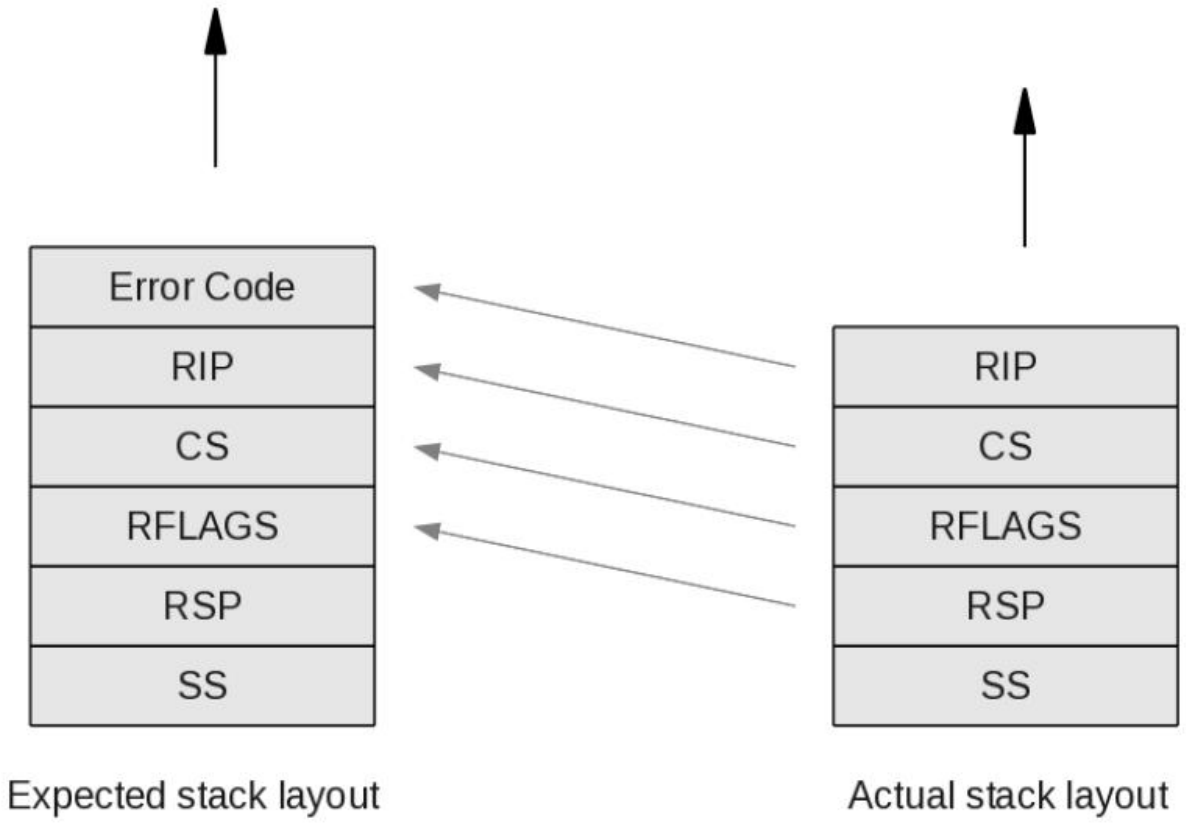
SIPI


CPU #0
(BSP)
CPU #1
(AP)
CPU #2
(AP)
CPU #3
(AP)
vv000h
shellcode
SIPI
NIC
Malware
Untrusted
Driver Domain
(e.g. NetVM)
System Memory

Инъекция syscall



Инъекция #AC


Error Code
RIP
CS
RFLAGS
RSP
SS
RIP
CS
RFLAGS
RSP
SS
Expected stack layout
Actual stack layout

Аппаратная виртуализация и вредоносное ПО

- Виртуализация
- Добрые и злые гипервизоры
- Обнаружение гипервизоров и атаки на них
- **Противодействие обнаружению**
- Перспективы

Противодействие обнаружению

- Как не дать себя обнаружить:
  - Подготовиться заранее
  - Быть начеку и контратаковать
  - Убрать улики и удалиться

Противодействие обнаружению

- Как не дать себя обнаружить:
  - Подготовиться заранее
  - Быть начеку и контратаковать
  - Убрать улики и удалиться

Противодействие обнаружению

- Стратегия 0
  - Пытаться знать обо всех мыслимых способах обнаружения
  - Держать в коде гипервизора контрприемы к ним
- Выиграет тот, у кого глубже уровень рефлексии
- С уровнем рефлексии объем кода очень сильно растет

Противодействие обнаружению

- Стратегия 1
  - Ничего не писать на диск, жить только в памяти
  - Следить за подозрительными паттернами инструкций гостевой ОС
  - В случае чего – быстро выгрузиться из памяти
- Придумана в BluePill, называется BlueChicken
- Ее можно обойти ☺

Противодействие обнаружению

- Стратегия 2
  - Не реагировать на попытки обнаружения
  - Сфокусироваться на качестве (добрым)
  - Сфокусироваться на эффекте (злым)

Сравнительная характеристика атак

Тип метода обнаружения	Сложность реализации атаки	Сложность реализации противодействия	Целесообразность реализации атаки	Целесообразность реализации противодействия	Вероятность атаки	Вероятность противодействия
Особенности (CPU bugs)	высокая	высокая	низкая	низкая	низкая	средняя
Вложенность виртуализации	высокая	средняя	средняя	средняя	средняя	высокая
Таймеры	низкая	низкая	средняя	высокая	высокая	высокая
Профилирование	средняя	высокая	высокая	высокая	высокая	средняя
Синхронизация	низкая	высокая	высокая	средняя	средняя	средняя
Уязвимости	наивысшая	средняя	средняя	высокая	средняя	высокая

Аппаратная виртуализация и вредоносное ПО

- Виртуализация
- Добрые и злые гипервизоры
- Обнаружение гипервизоров и атаки на них
- Противодействие обнаружению
- **Перспективы**

Перспективы

- Недостатки РПС-гипервизоров
  - Сложность разработки:
    - BluePill – 4 человек*месяц для базовой функциональности гипервизора
      - По оценка авторов, еще до 1 человек*года для реализации маскировки и вредоносной функциональности
  - Сложность сокрытия самого наличия режима виртуализации

Перспективы

- Да и зачем, разве мало РПС типа 0-2?

Перспективы

- Да и зачем, разве мало РПС типа 0-2?

Перспективы

- Доверенный, одобренный производителем аппаратуры гипервизор, загруженный первым – это почти панацея. Еще есть TPM.
- Просить пароль при входе в режим VMX
- Просто отключить

Перспективы

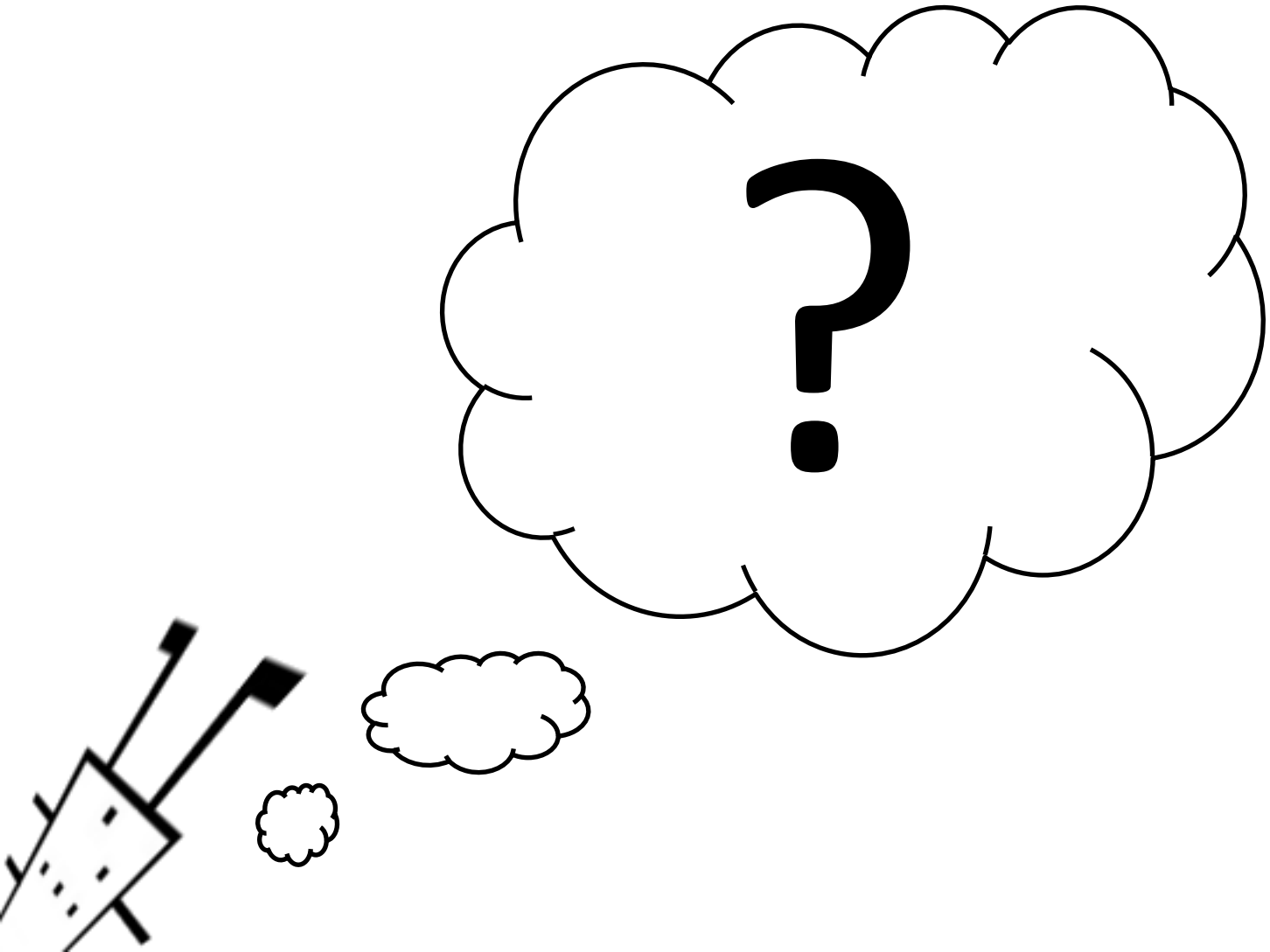
- Доверенный, одобренный производителем аппаратуры гипервизор, загруженный первым – это почти панацея. Еще есть TPM.
- Просить пароль при входе в режим VMX
- Просто отключить

Перспективы

- Добрые гипервизоры нужны и будут процветать
- Следует ожидать:
  - Полноценных средств защиты с поддержкой HVM
  - Гипервизоров, надежно изолирующих гостевые среды
    - Qubes?

Перспективы

- Атаки на уязвимости в легитимных гипервизорах
  - Сложно искать
  - Сложно эксплуатировать
  - Привязка к оборудованию



Keywords

Intel: VT-x, VT-d, EPT

AMD: AMD-V, SVM, IOMMU, NPT, RVI

bluepill, bitvisor, hyperdbg