САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ. ВИРТУАЛЬНАЯ БЕЗОПАСНОСТЬ ИЛИ БЕЗОПАСНАЯ ВИРТУАЛИЗАЦИЯ?

Д. т. н., профессор, заведующий кафедрой
«Информационная Безопасность Компьютерных Систем»
Зегжда Петр Дмитриевич
Д. т. н., профессор Зегжда Дмитрий Петрович
Каретников Алексей Валерьевич

Сравнение платформ облачных вычислений

	Ubuntu	VMware	Microsoft	Xen
Архитектура	Иерархическая	Централизованная	Гибридная	Децентра-лизованная
Поддерживаемые гипервизоры	KVM/XEN	ESX/ESXi	Hyper-V/ ESX/ESXi	XEN
Поддержка миграции ВМ	Нет	Без перезагрузки	Без перезагрузки	Без перезагрузки
Нужен доступ к рабочим узлам из внешней сети	Нет	Нет	Нет	Да
Механизм идентификации пользователей	Rsa-key	vClient (login:pass)	AD (login:pass)	ResPool (login:pass)
Динамическая балансировка нагрузки	Нет	Есть	Есть	Нет
Популярность (доля рынка)	5%	30%	20%	15%

Инциденты безопасности в облачных системах в 2011 году

	Инцидент
Апрель	Сбой Amazon Web Services (AWS) затронул тысячи пользователей.
Апрель	В результате атак на сервера Sony Computer Entertainment сервис был отключен. Личные данные пользователей, включая номера кредитных карт, возможно, были похищены.
Март	Недоступность сервиса Heroku – популярной облачной PaaS платформы.
Март	Проблемы в отказе IaaS сервисов в GoGrid.
Февраль -Март	Многочисленные проблемы пользователей сервиса Twitter при отправке сообщений, получения уведомлений, определения местоположения, поиска и других функций.
Февраль	Проблемы пользователей Rackspace при работе с почтой.
Январь	Часть клиентов испытывали проблемы с доступом к пакету Microsoft Business Productivity Online Suite (BPOS). Сервисами BPOS пользуются крупнейшие мировые компании, в том числе департамент сельского хозяйства США, который планирует перевести 120 000 сотрудников на облачные сервисы Microsoft BPOS.

Основные проблемы мешающие развитию облачных вычислений по мнению пользователей

Проблемы	Для малого бизнеса	Для среднего бизнеса
Безопасность данных, обрабатываемых в облака	**50%**	**47%**
Постоянные выплаты поставщику облачных услуг	42%	27%
Облачные приложения не принадлежат пользователям облака	37%	31%
Надежность предоставления услуги	24%	23%
Потеря контроля за обработкой информации в облаке	18%	21%

IDC Analyze the Future

Для каждой проблемы в таблице указан процент опрошенных, назвавших эту проблему наиболее важной

Специфика облачных вычислений с точки зрения безопасности

- Хранение данных у незаинтересованной стороны
- Контроль и управление безопасностью по требованию
- Выявление нарушений в реальном времени
- Быстрое восстановление работоспособности сервисов
- Расширенные возможности по организации приманок (Honey-Net)
- Необходимость подготовки квалифицированных специалистов по безопасности облачных систем
- Значительные инвестиции в инфраструктуру безопасности

Классы атак для систем облачных вычислений

- Традиционные атаки на ПО
- Атаки на клиента
- Атаки на средства виртуализации
- Реализация комплексных угроз

Атаки на клиента

Пользователи работают с сервисом облачных вычислений с помощью Интернет-браузера, поэтому подвержены традиционным атакам:

- Cross site scripting (XSS)
- ARP-spoofing
- DNS-spoofing
- SSL injection
- Fishing
- Viruses, Trojans, Rootkits

Атаки на облако с использованием средств виртуализации

- Атаки на гипервизор
- Атаки на средства взаимодействия между узлами облака
- Атаки на системы управления облаком

Атаки на гипервизор

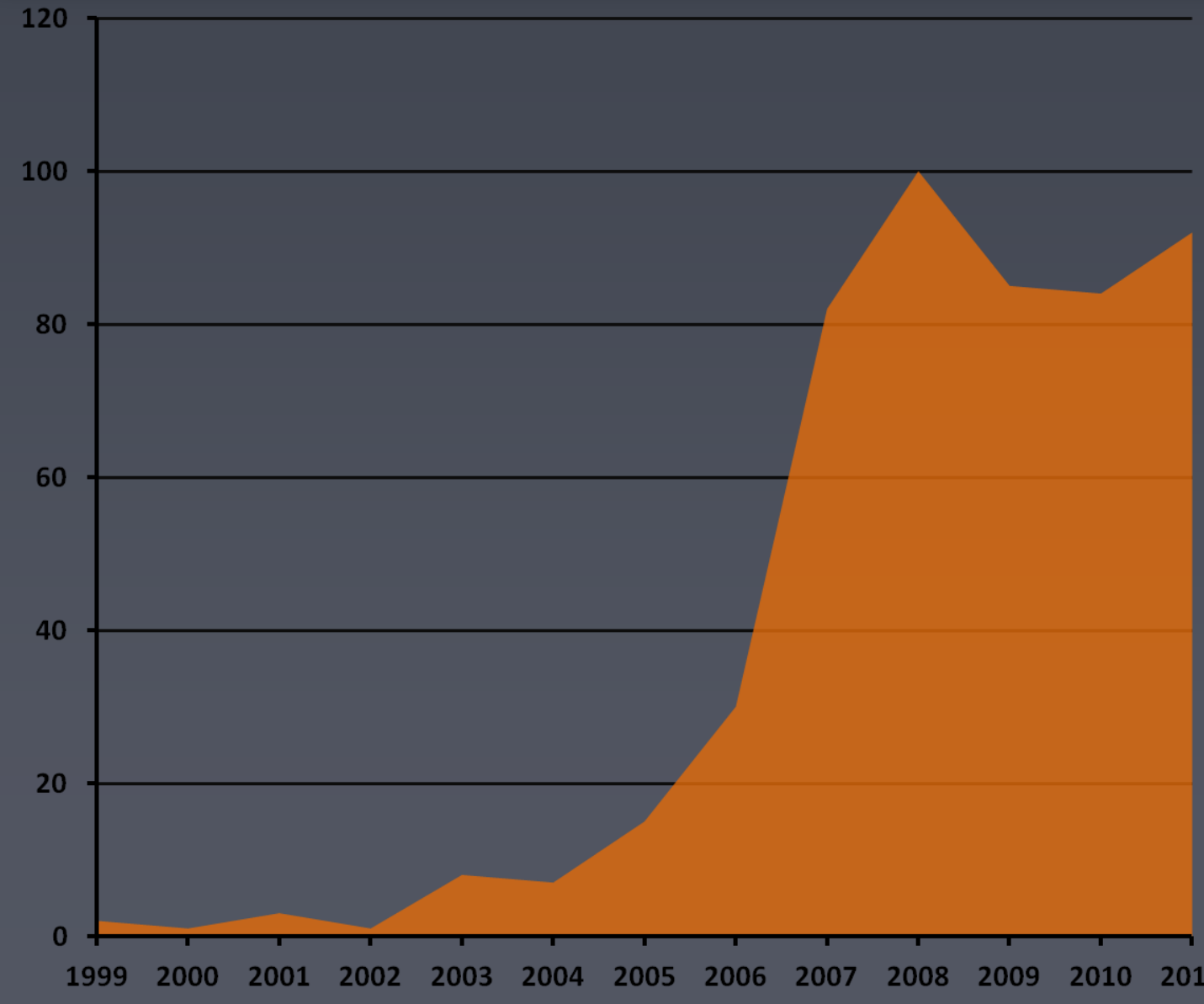
Атаки на гипервизор

Изоляции памяти ВМ подвержена атакам и уязвимостям

Атаки на средства взаимодействия между узлами облака

Интерфейсы виртуальных устройств подвержены целенаправленному воздействию со стороны высококвалифицированного нарушителя

Уязвимости в средствах виртуализации



Всего

553

уязвимости

По данным
IBM XForce

Классификация уязвимостей средств виртуализации

Класс	Описание	Процент от общего числа уязвимостей
Воздействие на гипервизор	Нарушение работы гипервизора, внедрение кода в гипервизор	38%
Выход за пределы ВМ	Нарушение изоляции ВМ, внедрение кода в другие ВМ или гипервизор	35%
Воздействие на гостевую ОС	Нарушение работы гостевой ОС, внедрение кода в гостевую ОС	15%
Прочие	Нарушение работы средств управления средств виртуализации, нарушение работы вспомогательных программ	12%

По данным IBM XForce

Примеры уязвимостей

- CVE-2011-4127 – уязвимость найденная в 2011 году. Эта уязвимость позволяет пользователям ВМ читать и изменять данные на всем жестком диске физического компьютера, в том числе можно изменять код и данные гипервизора и других ВМ.
- CVE-2011-1751 – уязвимость найденная в 2011 году. Эта уязвимость позволяет пользователям ВМ выполнить произвольный код в контексте хостовой ОС.
- CVE-2011-1872 - уязвимость найденная в 2011 году. Эта уязвимость позволяет пользователям ВМ вывести из строя весь узел, на котором работает эта ВМ и гипервизор.
- Во время осуществления миграции ВМ с одного узла на другой, данные оперативной памяти ВМ передаются по внутренней сети провайдера в открытом виде.

Комплексная атака на систему облачных вычислений

1. Атака на ВМ из внешней сети
   - Запуск кода внутри ВМ
2. Выполнение кода в ядре ОС в ВМ
   - Взаимодействие с виртуальным оборудованием напрямую
3. Выполнение кода в гипервизоре
   - Атака на другие ВМ на том же узле сети
   - Выполнение кода на узле внутренней сети облака
4. Прослушивание траффика внутренней сети облака
   - Прослушивание данных пользователей
   - Получение доступа к другим ВМ в облаке
   - Модификация данных ВМ
5. Выполнение DoS атак на другие узлы и ВМ
   - Запуск механизмов самовосстановления облака
   - Инициация механизмов миграции ВМ
6. Атаки на системы управления облаком
   - Получение контроля за всем облаком

Анализ защищенности внутреннего трафика платформ облачных вычислений

Критерий	Ubuntu Enterprise Cloud	VMware vSphere	Microsoft System Center	Xen Cloud Platform
Управление узлами виртуализации	подпись	шифрование	подпись	шифрование
Передача оперативной памяти при миграции	нет миграции	не защищено	не защищено	не защищено
Взаимодействие с хранилищем данных	не защищено	шифрование	шифрование	не защищено

Критичные технические угрозы систем облачных вычислений

- Угроза захвата управления над облаком
  - Использование облака для решения задач нарушителя
- Угроза получения контроля над гипервизором
  - Получение доступа во внутреннюю сеть облака
  - Атаки на другие ВМ
- Угроза раскрытия и модификации трафика
  - Нарушение механизмов работы систем управления
- Угроза перехвата и модификации ВМ при миграции с одного физ. узла на другой
  - Захват и внедрение кода во множество ВМ
- Угроза нарушения границ изоляции ВМ
  - Внедрение кода в другие ВМ и гипервизор

Специфика защиты (1)

- Размывание обработки данных и необходимость выполнять международные нормы по защите данных:
  - Директива ЕС о защите данных(EU Data Protection Directive) и программа защиты данных США (U.S. Safe Harbor program)
  - Доступность данных иностранным правительствам и организациям
  - Проблема копирования данных (неуничтожение)
  - Трудность выполнения закона о Персональных данных
- Необходимость контроля за изоляцией
- Совместное владение инфраструктурой обработки данных
- Протоколирование работы
- Проблемы владения данными
- Обеспечение гарантированности сервисов

Специфика защиты (2)

- Зависимость от безопасности гипервизора
- Привлекательность для хакеров как объект атаки
- Безопасность виртуальных ОС
- Возможность массированных перебоев с энергией
- Криптография для распределенных вычислений
  - Криптографическая защита доступа к интерфейсу управления ресурсами облака/грид
  - Криптографическая защита доступа администратора к экземплярам виртуальных ОС
  - Криптографическая защита доступа к приложениям
  - Криптографическая защита данных приложений
- Недостаточность защиты публичных облаков по сравнению с частными
- Недостатки контроля версий приложений в публичных облаках

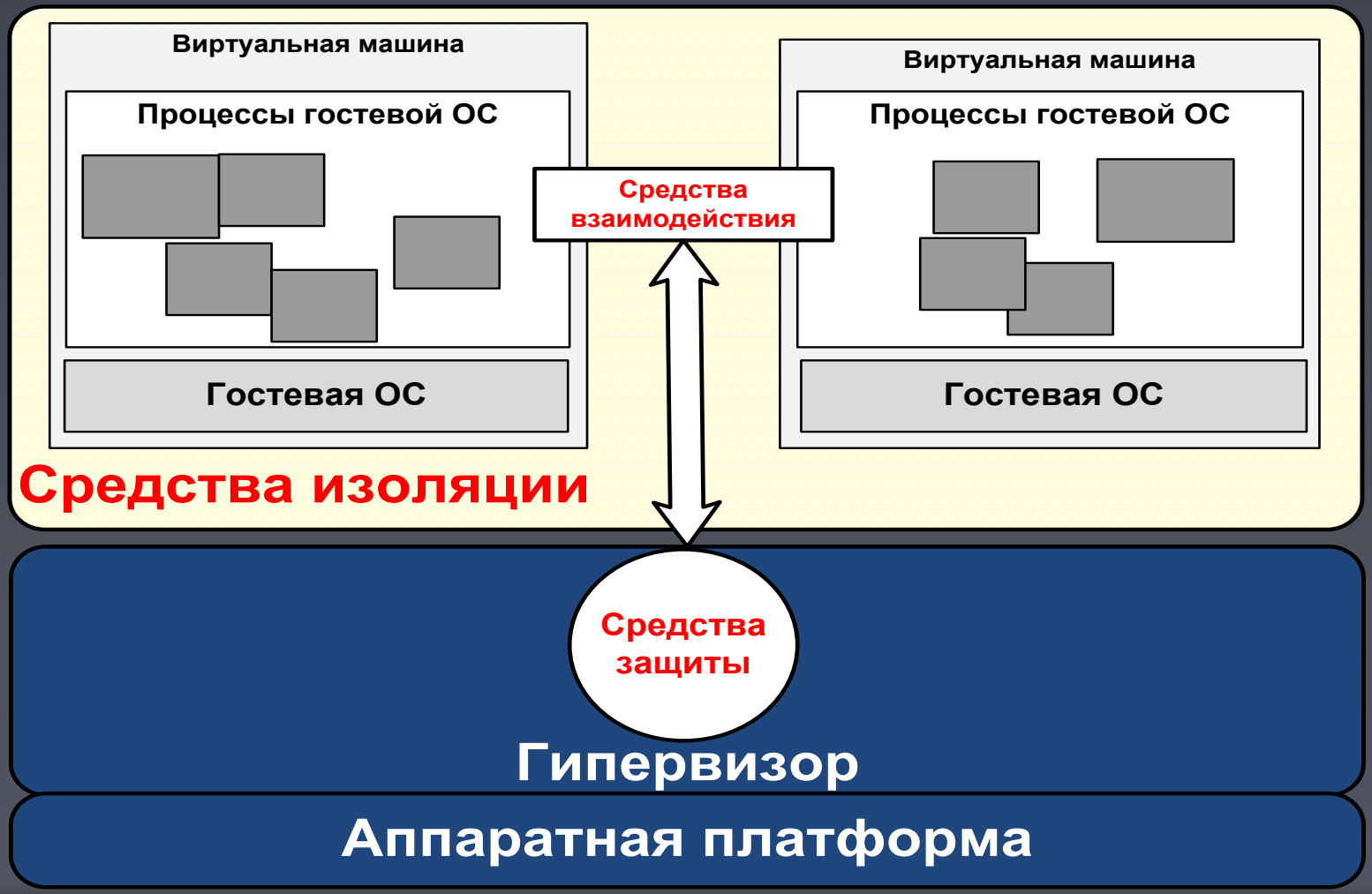
Эффективны ли стандартные средства защиты для облака?

Существующие средства защиты не предотвращают атаки на средства виртуализации из виртуальной машины

Комплексная атака на облако

После успешной атаки на средство виртуализации, нарушитель может успешно атаковать всю внутреннюю сеть облака

Гибридная система

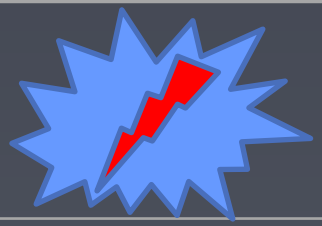


Если начинают с неправильного, то мало надежды на правильное завершение.
Конфуций

Виртуализация и угрозы безопасности

Направленность / Источник	Гипервизор	Средства виртуализации	Гостевая система
Внешняя среда			
Гипервизор			
Средства виртуализации			
Гостевая система			

Доверенный гипервизор

Направленность / Источник	Гипервизор	Средства виртуализации	Гостевая система
Внешняя среда			
Гипервизор			
Средства виртуализации			
Гостевая система			

Безопасность гостевой системы определяется безопасностью гипервизора и виртуализацией ресурсов

ГОСТЕВАЯ СИСТЕМА НАСЛЕДУЕТ СВОЙСТВА БЕЗОПАСНОСТИ ГИПЕРВИЗОРА ПРИ СОБЛЮДЕНИИ ОПРЕДЕЛЕННЫХ УСЛОВИЙ

Чем выше здание, тем глубже фундамент.
Томас Фуллер

СЦЗИ, кафедра ИБКС
ГОУ «СПбГПУ»

Санкт-Петербург, ул.Политехническая, д.29, Главное здание, к. 173

тел: +7(812) 552-64-89,
552-76-32

Web: http://ibks.ftk.spbstu.ru
E-mail: Zeg@ibks.ftk.spbstu.ru