Распределенные системы хранения и обработки данных

Владислав Белогрудов, EMC

vlad.belogrudov@gmail.com

EMC²

Лекция 10

Безопасность инфраструктуры хранения и облачных датацентров

EMC²

Содержание лекции

- Общие принципы
- Сети СХД
- Облачная инфраструктуры
- Виртуальная среда
- Управление пользователями и правами доступа

Риски

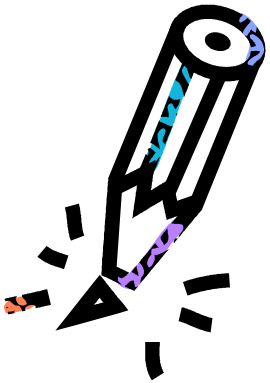
- Сочетание вероятности и последствий наступления (не)благоприятных событий
- Безопасность – попытка уменьшить убытки
- Невозможно полностью избежать риски

Риски = Угрозы X Уязвимости

Угрозы

- Предполагаемая опасность, но не всегда атака
- Основные угрозы
  - Вирусы, руткиты, ..
  - Работники
  - Землетрясения, пожары, наводнения
  - Терроризм
  - Эпидемии
- Чему угрожают?
  - Интеллектуальной собственности, бизнесу, ..

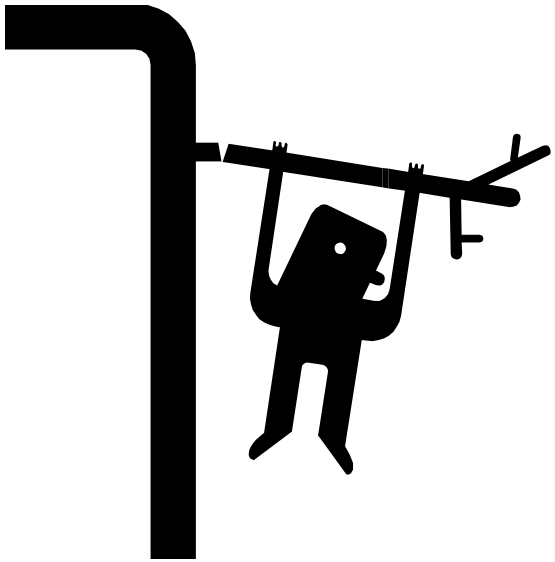
Уязвимости



- Слабые места
- Всегда будут в сложных системах
- Большая часть проблем – плохие программы
- Три типа
  - Известные
  - Неизвестные
  - Нулевого дня (zero day)

Триада риска

- CIA
  - Confidentiality
  - Integrity
  - Availability



Конфиденциальность

- Анализ траффика
- Интеллектуальная собственность
- Шифрование
- Скрытые каналы (стеганография и т.п.)
- Логические выводы

Целостность

- Модификации данных не могут быть произведены неавторизованными людьми и системами
- Неразрешенные модификации не могут быть произведены авторизованными людьми и системами
- Данные должны быть согласованы снаружи систем и внутри и снаружи

Инфраструктура безопасности

Служба ведения учета	Служба доступности
Служба целостности	Служба конфиденциальности

Службы безопасности

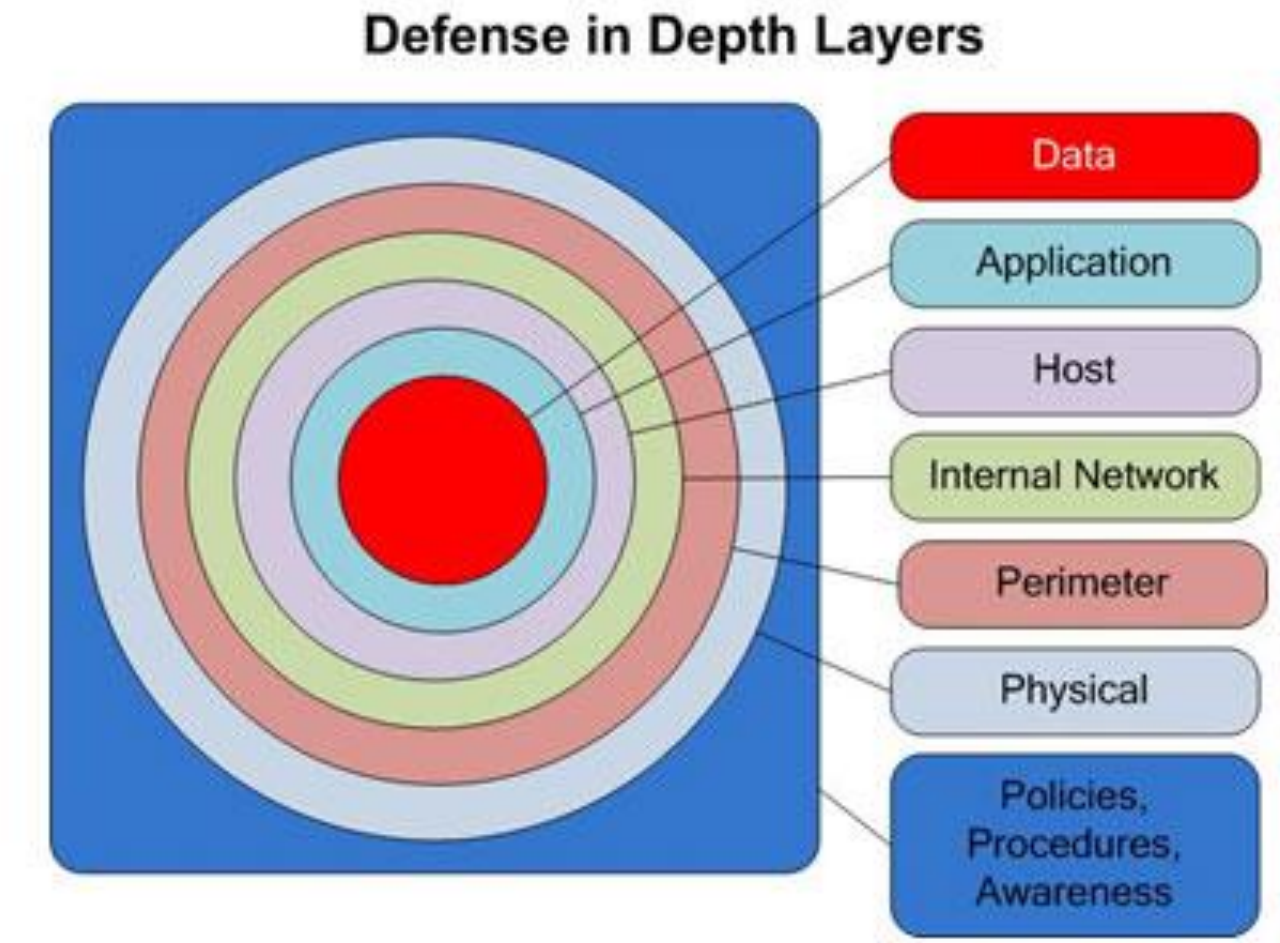
Атака	Конфиден-циальность	Целостность	Доступность	Отчетность
Доступ	X			
Изменение	X	X		X
Отказ в об-служивании			X	
Отказ от авторства		X		X

Глубокая защита

- Defense in Depth
  - Все точки системы

- Виды
  - равномерная защита
  - островки безопасности
  - фокус на данных
  - вектор атаки

Уровни защиты

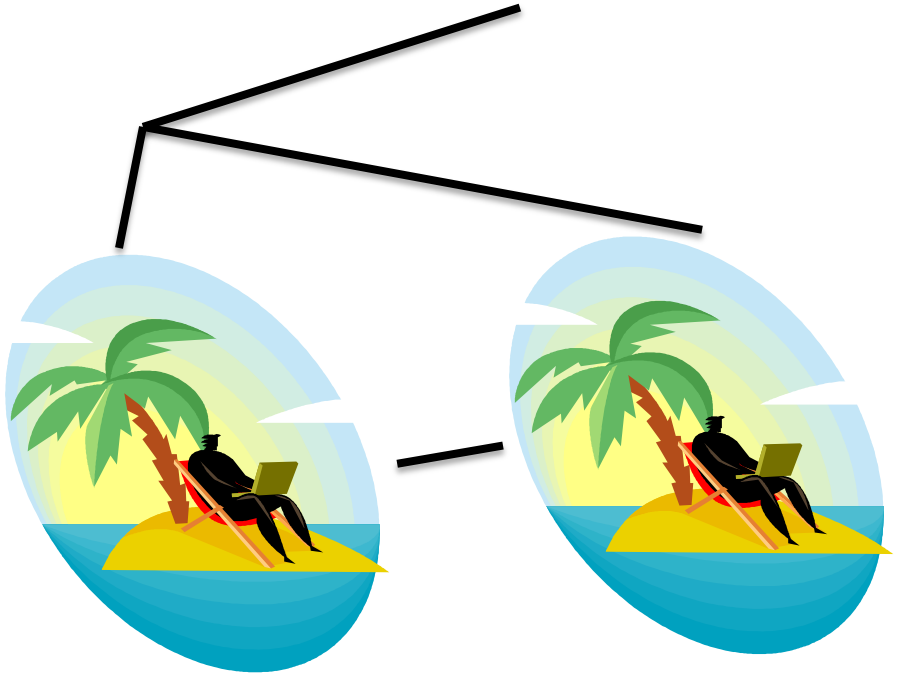


Равномерная защита

- Используется чаще всего
- Все системы одинаково важны
- Особенно уязвима инсайдерским атакам
- Firewalls, VPN, IDC/IPS, Antivirus, etc.

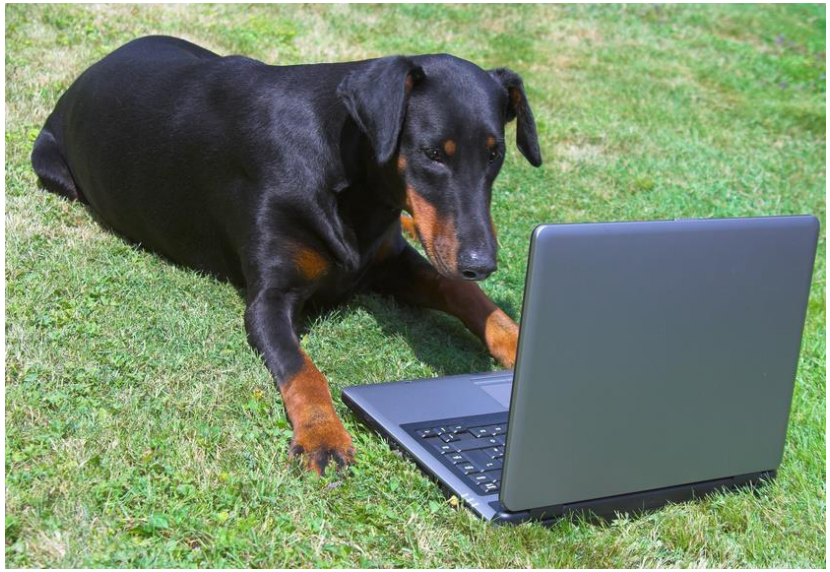
Островки безопасности

- Сегментация сети
- Ограничение доступа к критическим сегментам
- Использует
  - VPN
  - Internal Firewalls
  - VLAN, ACL



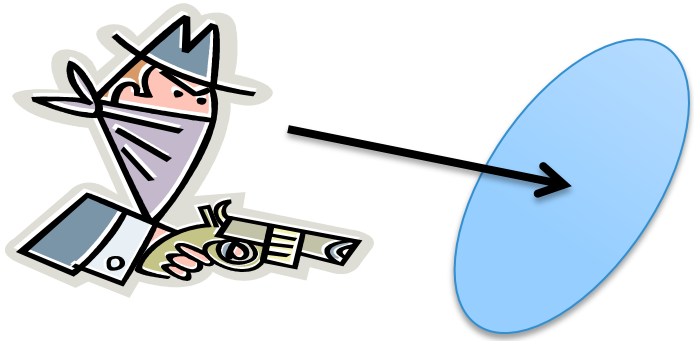
Фокус на данных

- Идентификация и классификация данных
- Различные уровни доступа
- Защита данных на уровне приложений
- Защита хостов и сети



Векторы и области атаки

- Область атаки – слабое место системы
- Вектор атаки – необходимые действия



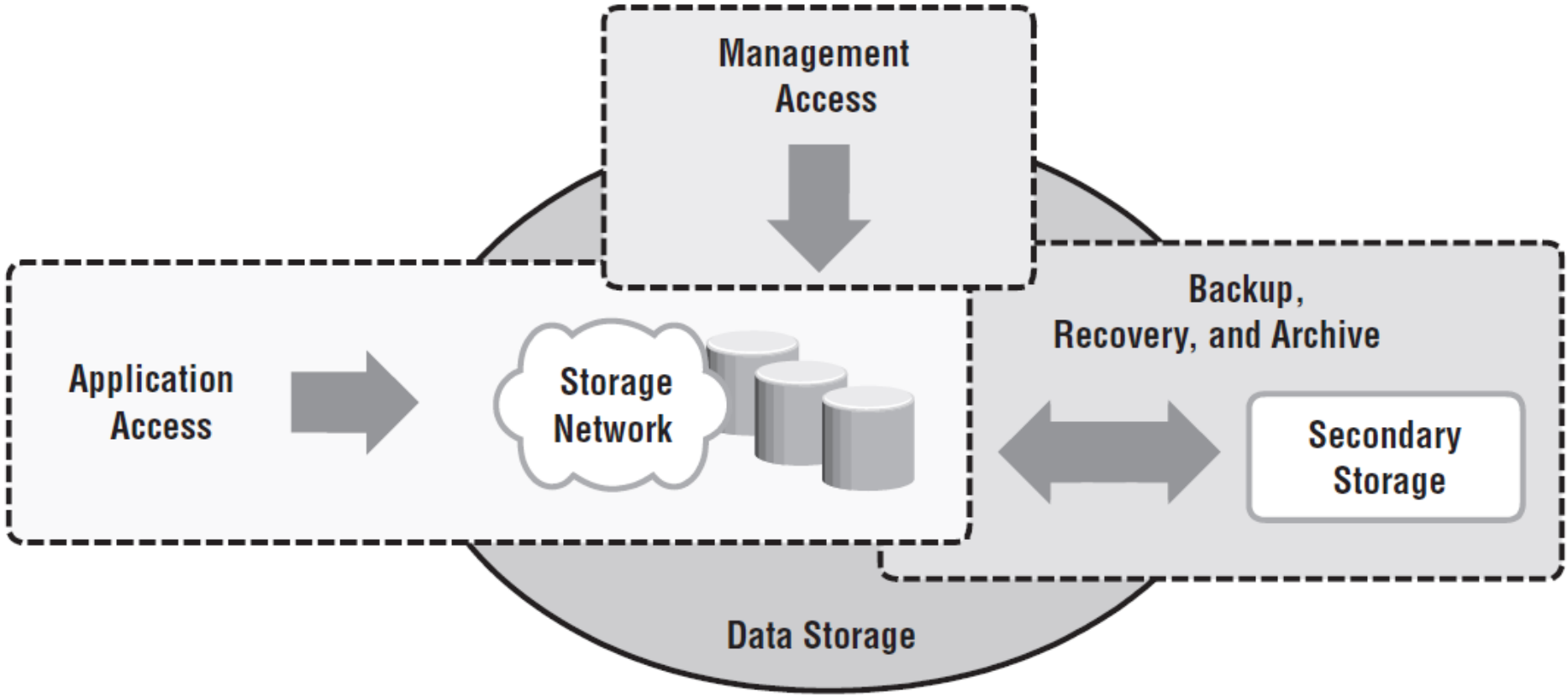
Например:

USB drive =>

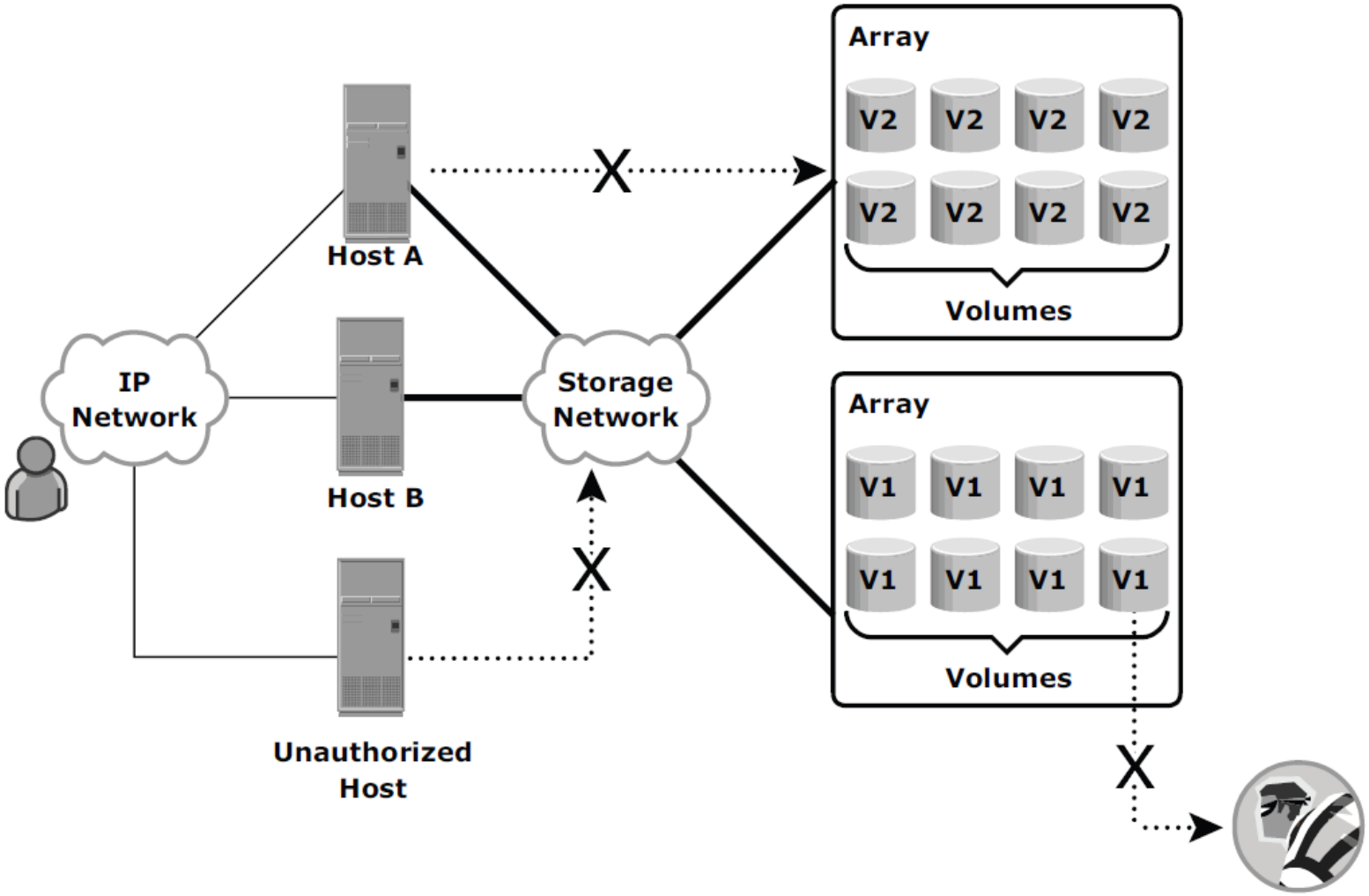
разносчик вирусов =>

заблокировать ☺

Безопасность инфраструктуры хранения – области защиты

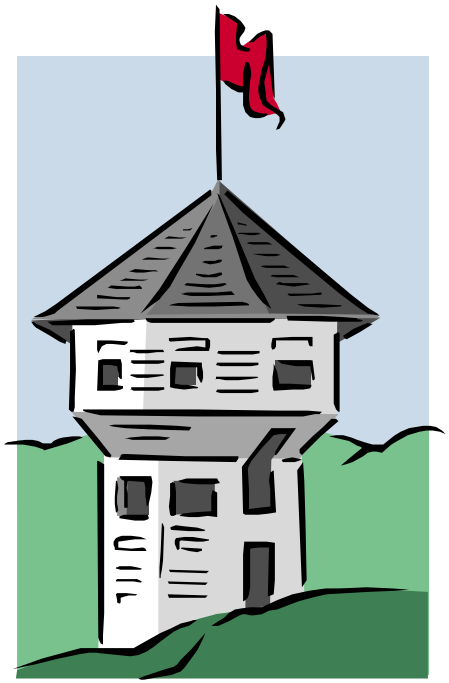


Угрозы в сетях хранения

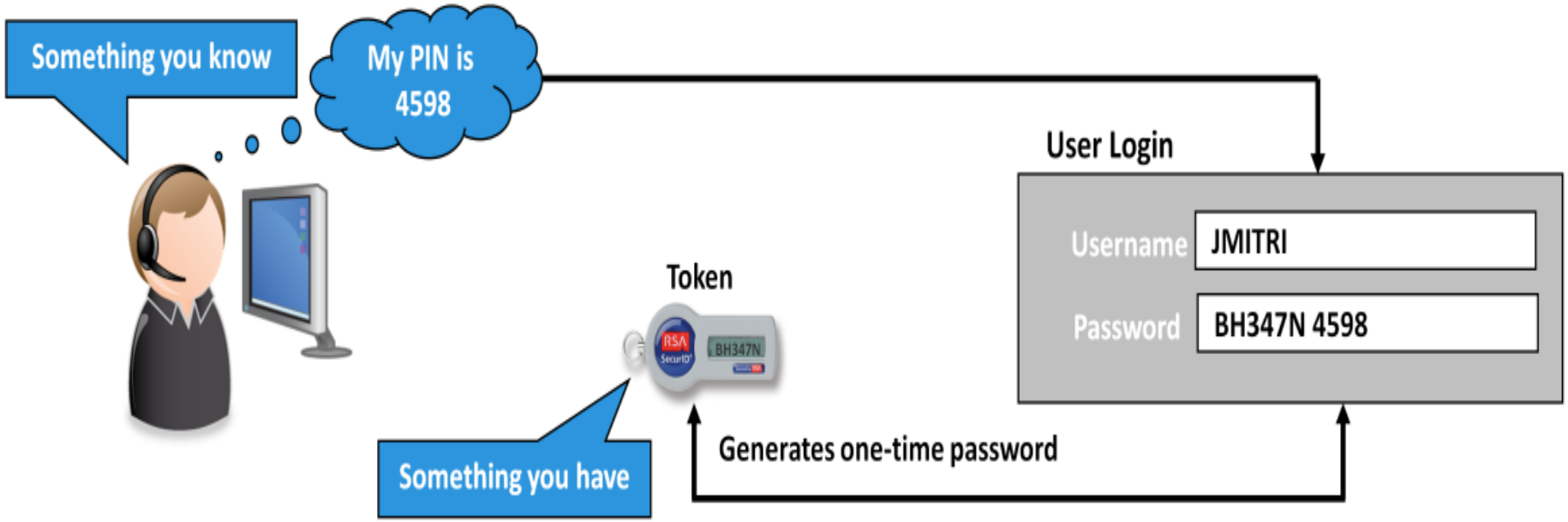


Техники защиты в сетях хранения

- IP
  - VLAN
  - VPN
  - SSL
  - CHAP
- SAN
  - LUN masking
  - Zoning
- NAS
  - LDAP
  - Kerberos



Многофакторная аутентификация



Облачная инфраструктура – источники угроз

Основные угрозы

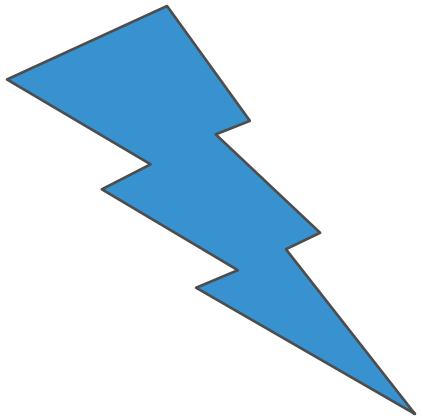
Коммунальность

Потеря контроля

- Данные
  - в покое
  - в движении
  - в обработке

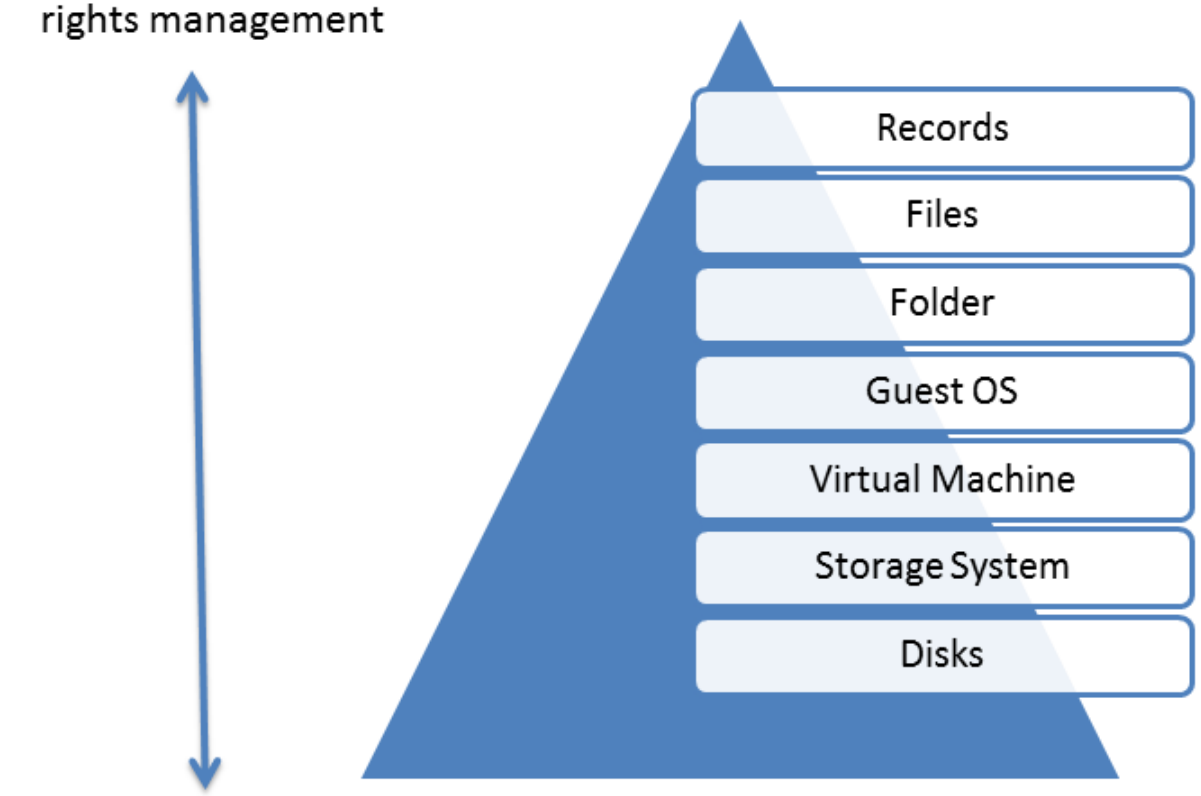
Облачные риски

- Неавторизованный доступ персонала и соседей:
  - дыры в гипервизоре
  - совместное использование ресурсов
- Lock-in
- Ограничение доступа
  - «шумные» соседи
  - сбои оборудования
- Подделка данных
- Жизнь данных после уничтожения



Шифрование – ключ к успеху?

data classification,
rights management



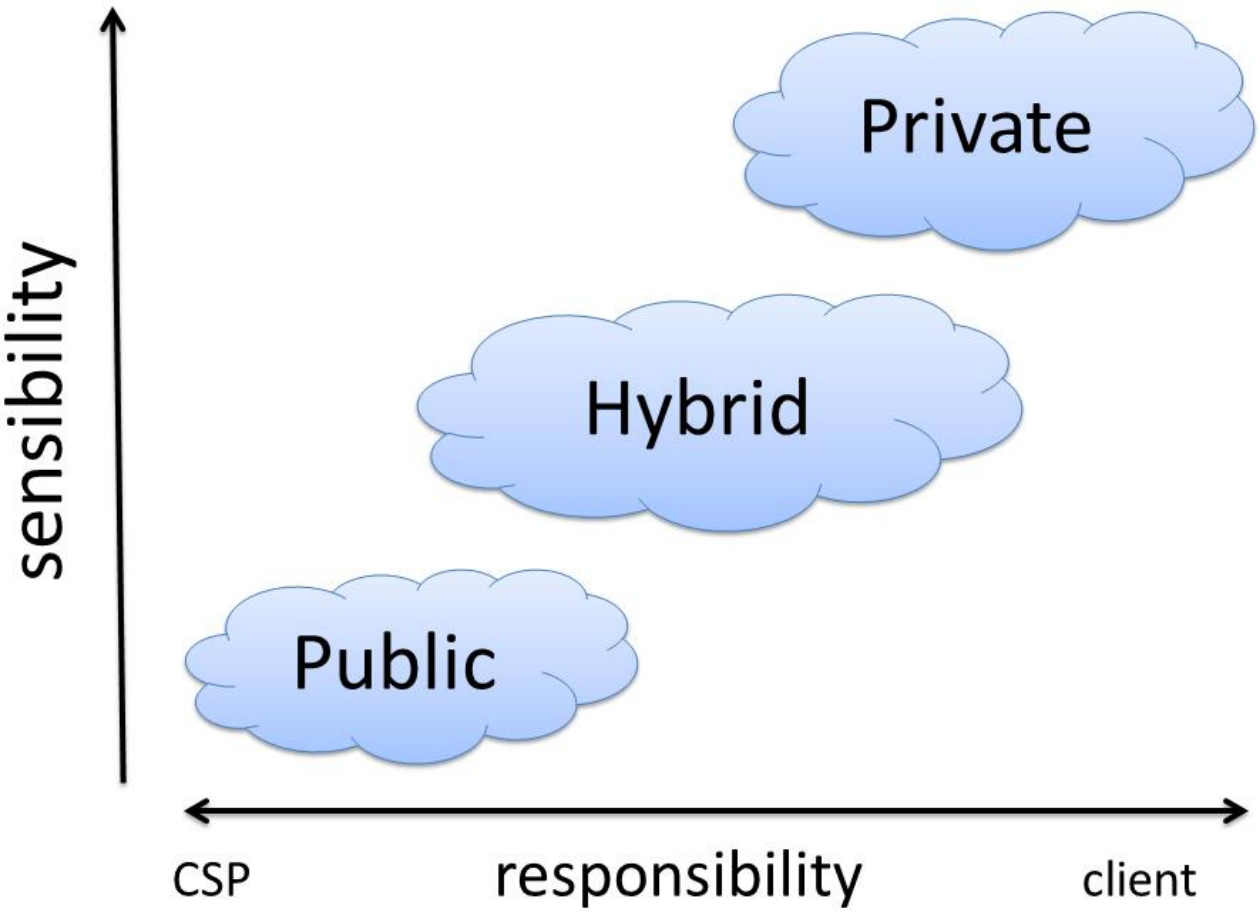
ease of use,
often more processing

Управление ключами и шифрованием

- Ключи и данные – раздельно
  - Свой сервер
  - Security as a Service в другом облаке
- Шифруем все
  - Не нужно классификации данных
  - Наиболее нежелательно для CSP (провайдера): дедупликация, компрессия, автоматизация
- Чем дальше от железа, тем больше работы
- Чем ближе к SaaS, тем меньше шансов шифровать самим пользователям

EMC²

Ответственность в облаках



Лучшие практики - CSA

- Cloud Security Alliance
  - Cloud Computing Architectural Framework
  - Information Management and Data Security
  - Interoperability and Portability
  - Traditional Security, BC/DR
  - Data Centre Operations
  - Incident Response
  - Application Security
  - Encryption and Key Management
  - Identity, Entitlement, and Access Management
  - Virtualization …

Лучшие практики - ENISA

- European Network Information and Security Agency
  - европейская организация по борьбе с кибер-преступностью
  - центр экспертизы

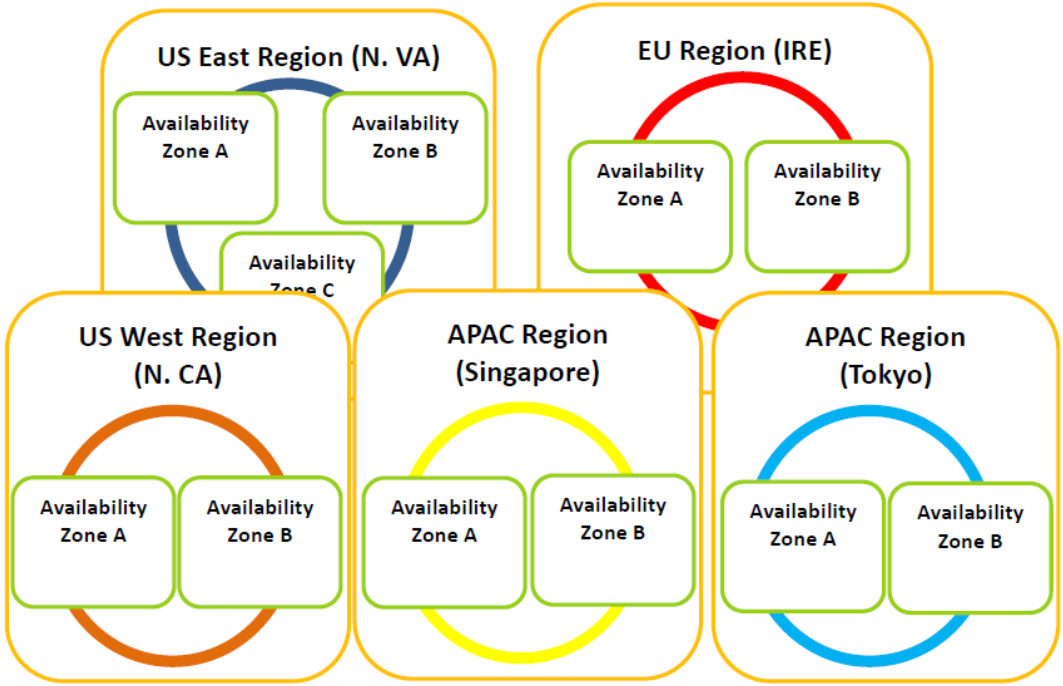
- "Cloud Information Assurance Framework"
  - «Опросник» для определения безопасности облака провайдера
- "Cloud Computing Security Risk Assessment"
  - рекомендации

Cloud Information Assurance Framework

- Персонал, субподрядчики
- Операции
  - backup, host, network, change control..
- Управление правами и доступом
- Управление активами
- Переносимость услуг (portability)
- Непрерывность бизнеса
- Физическая безопасность
- Законность

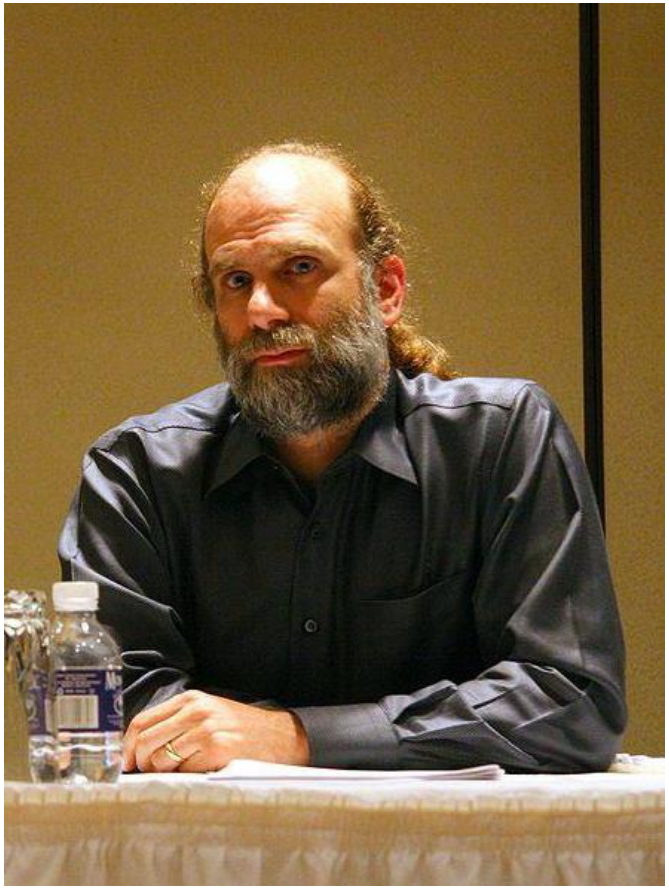
Amazon Web Services Security

- Security Whitepaper



Доверие облачным провайдерам

- Доверяем - пользуемся
- Облачные сертификации
- Schneier on Security (blog)
- Bruce Schneier on security for cloud computing (video)



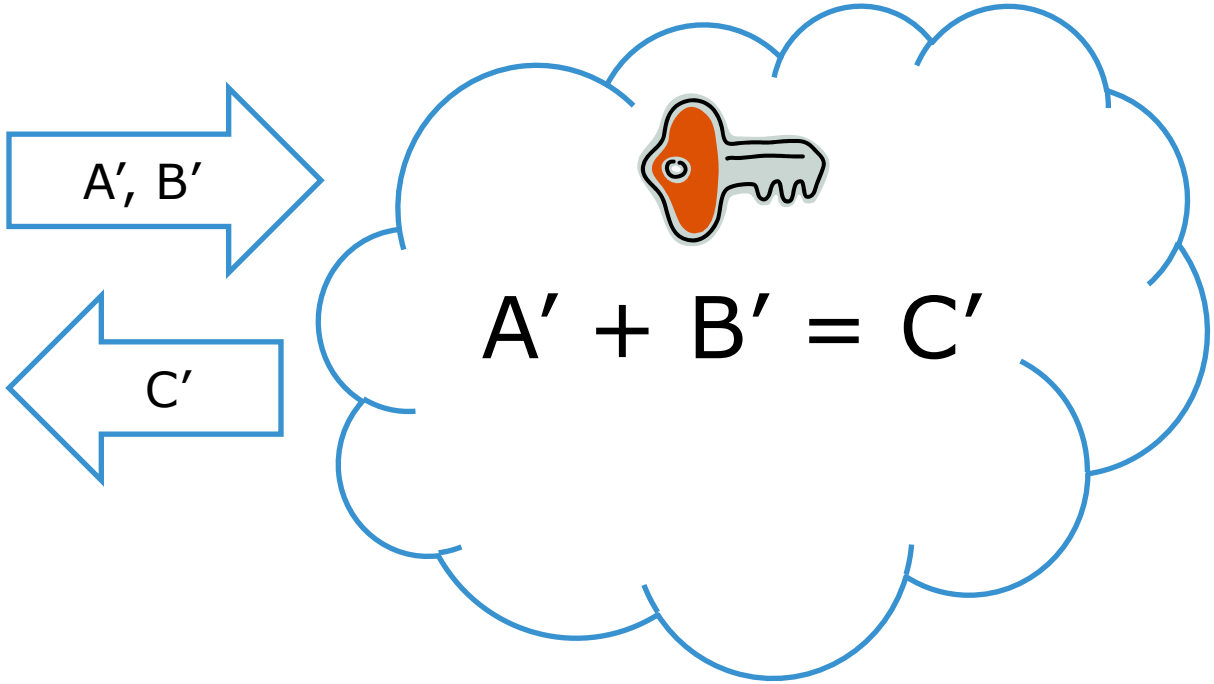
Технологии будущего

- Гомографические вычисления
  - secure multiparty computations

A+B=?

A -> A′
B -> B′

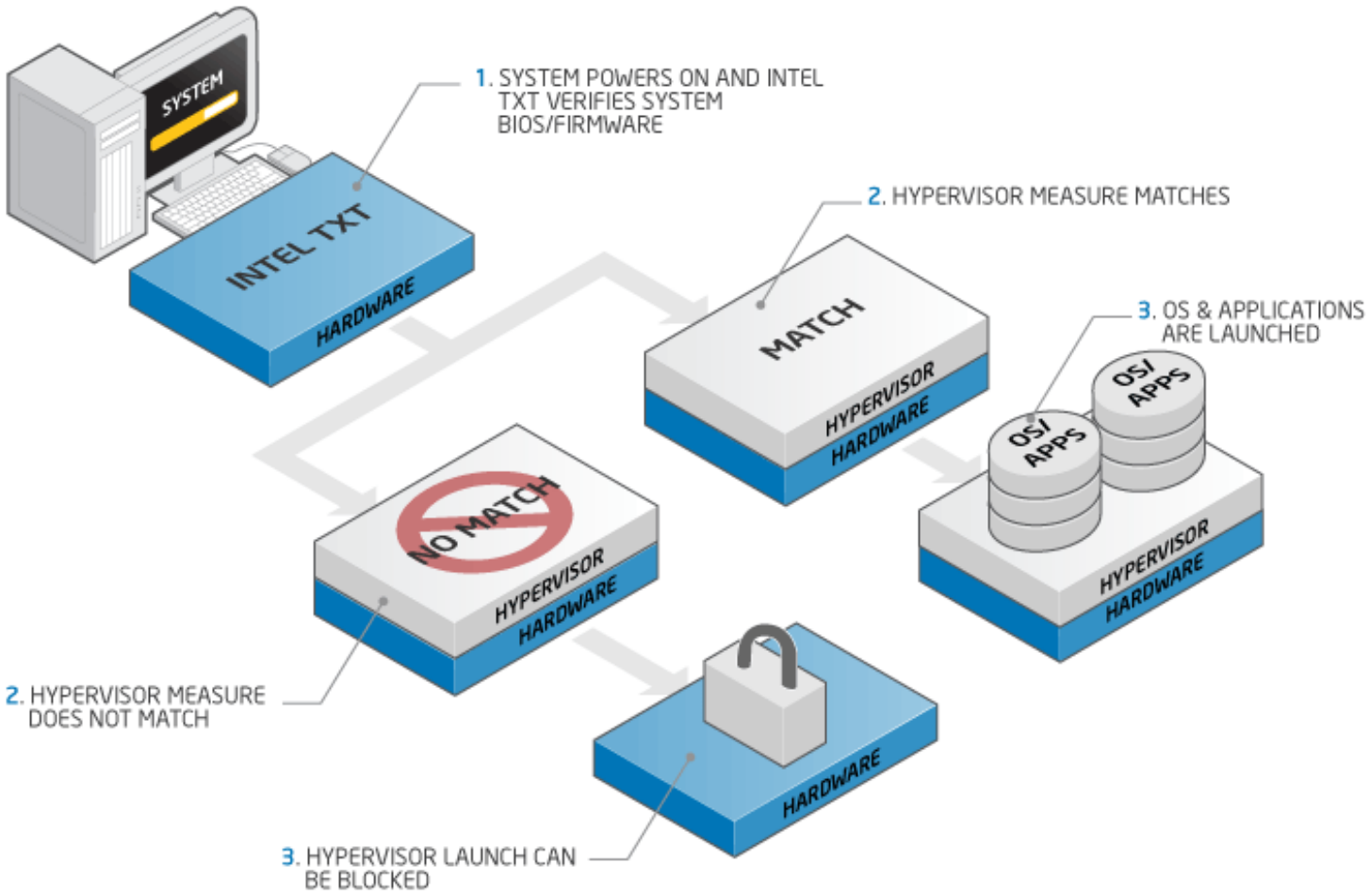
C′ -> C



Виртуальная среда - угрозы

- Гипервизор – черные ходы
- Обнаружение ВМ (VM Detection)
- Специфичные для ВМ бреши (VM exploits)
- Побег из ВМ (VM escape)
- Хатотичный рост числа ВМ (VM Sprawl)
- Недостаточная видимость происходящего
- Слишком большие права и привилегии
- Отсутствие физических барьеров

Intel Trusted Execution Technology



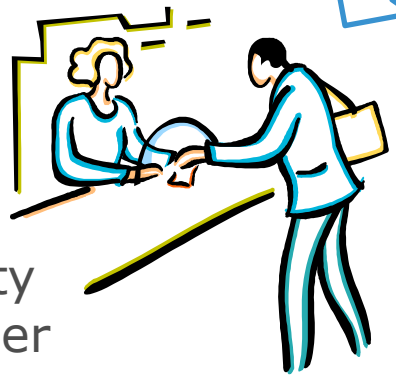
Управление правами и доступом

- SAML
- OpenID
- OAuth
- OpenID Connect

Single Registration, Single Sign On ..

Service Provider /
Relying Party

user

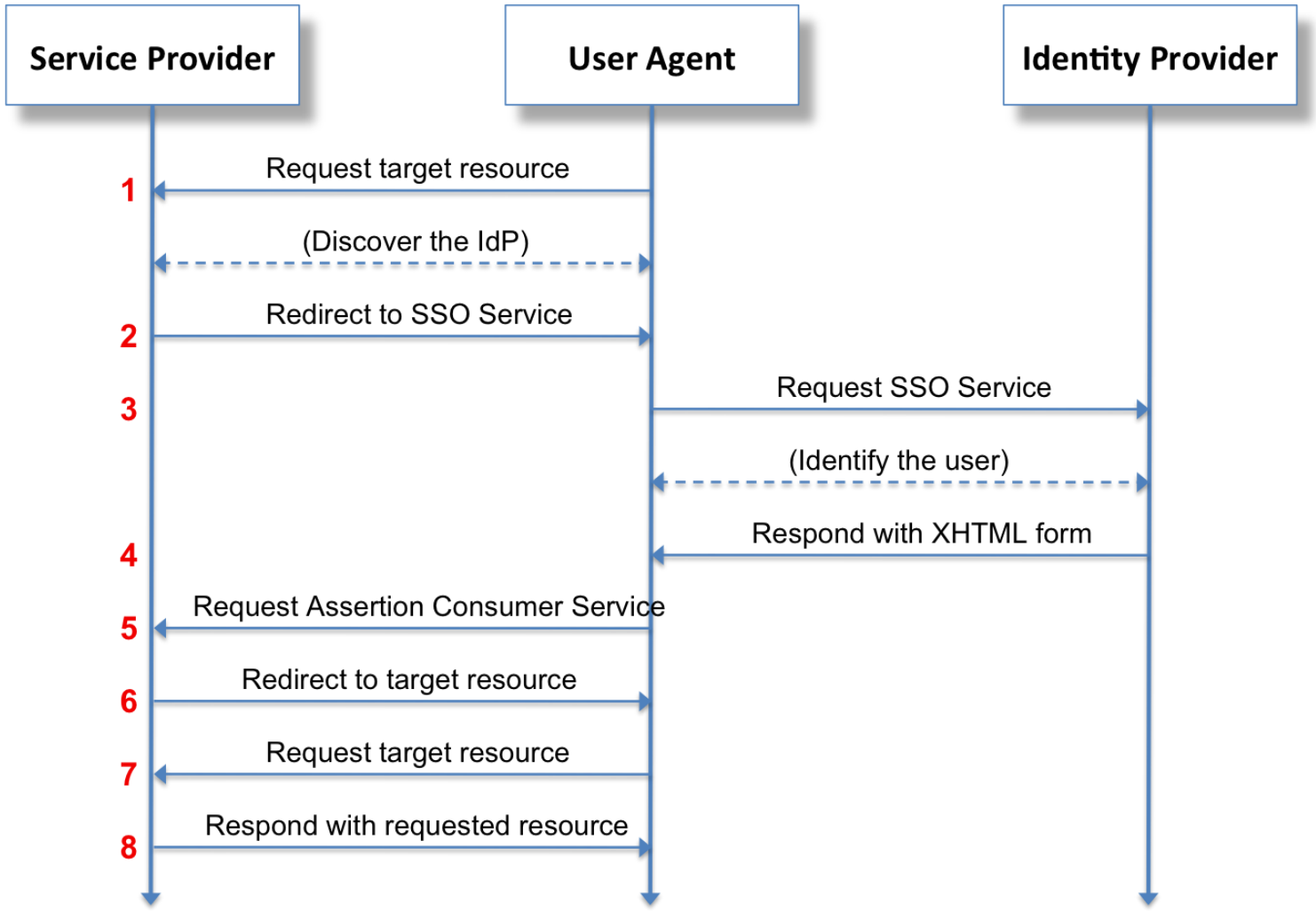


Identity
Provider

Security Association Markup Language

- SAML
  - «Язык разметки подтверждения безопасности»
- Обмен данными об аутентификации и авторизации между защищенными доменами
- Single Sign On
- XML
- SSL/TLS
- Используется организациями

SAML illustrated



OAuth – протокол авторизации

- Позволяет давать третьим лицам право доступа к данным без передачи логина и пароля
- Авторизация у своего провайдера
- Безопасно (? SSL)
- Удобно

Пример:

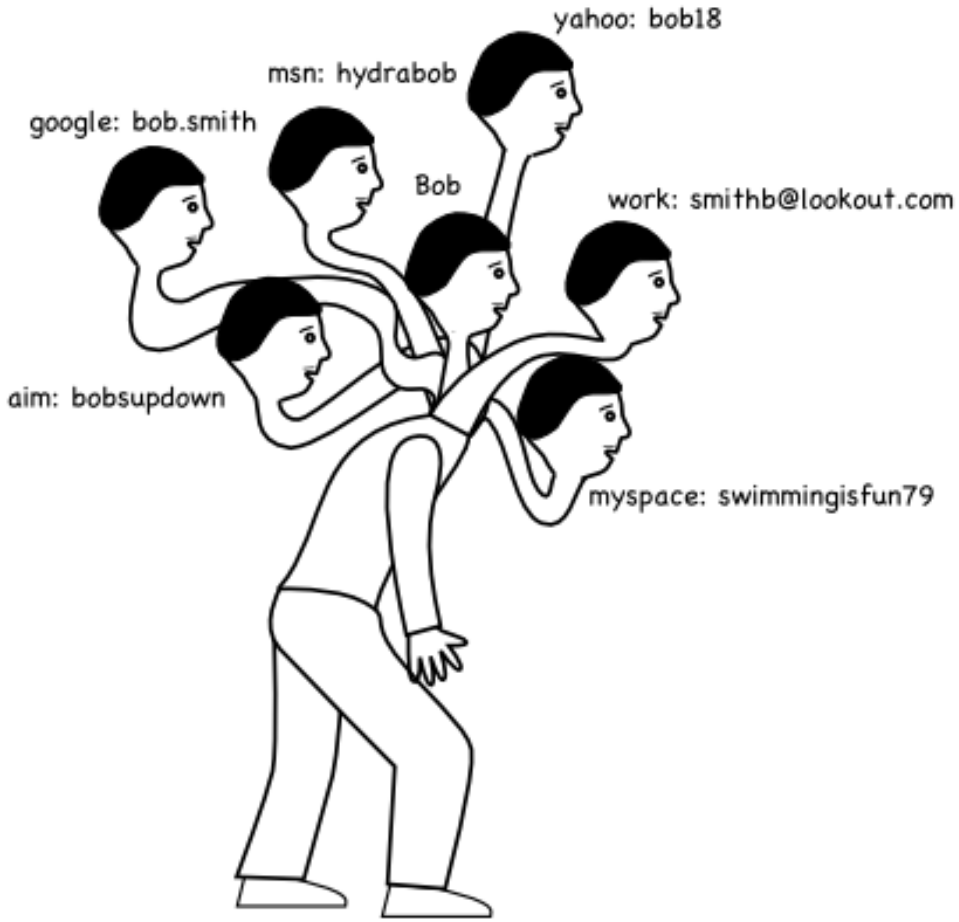
загрузка адресной книги

Gmail в Facebook

OpenID – открытая аутентификация

- Децентрализованная система учетных записей
- Провайдеры учетных записей (IdP)
  - Google, Yahoo!, PayPal, BBC, AOL, LiveJournal, MySpace, IBM, Steam, Sherdog, Orange, VeriSign
- Провайдер услуг (RP) перенаправляет аутентификацию в IdP
- Не нужно везде регистрироваться ☺

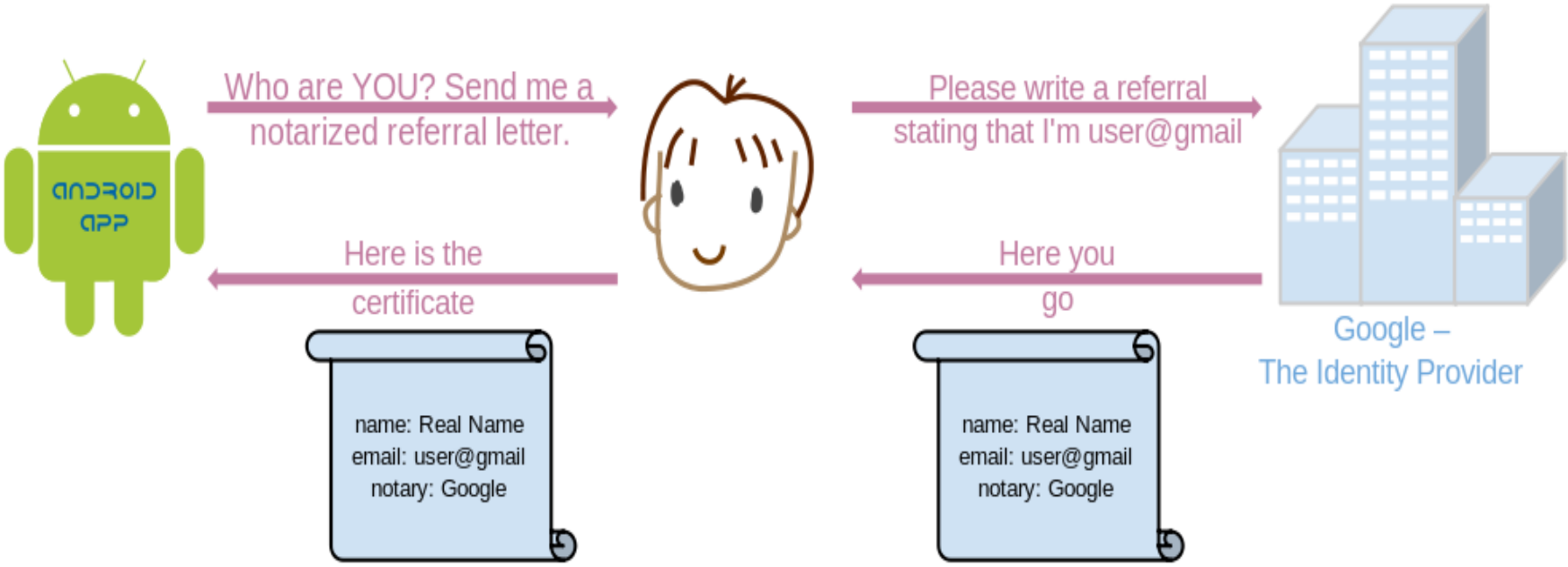
OpenID illustrated



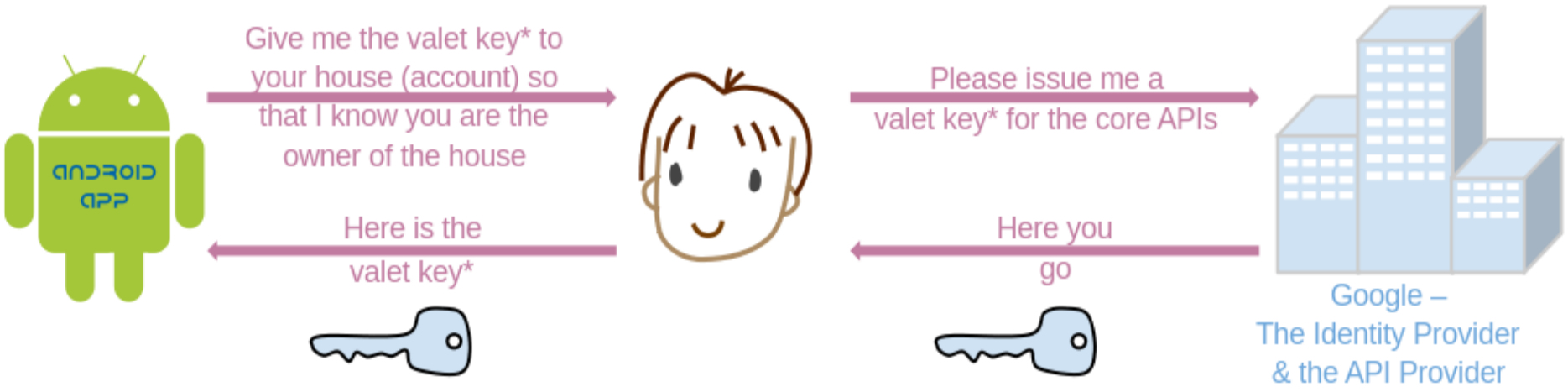
OpenID Connect

- простой протокол аутентификации и авторизации
- Jason/ReST
- OAuth 2.0 built-in / based on
- Обеспечивает различные уровни безопасности

OpenID vs Oauth - OpenID



OpenID vs Oauth - OAuth



Спасибо!

EMC²