# Безопасность в браузерах: Альтернативы SSL

Алексей Хлебников

LVEE 2017

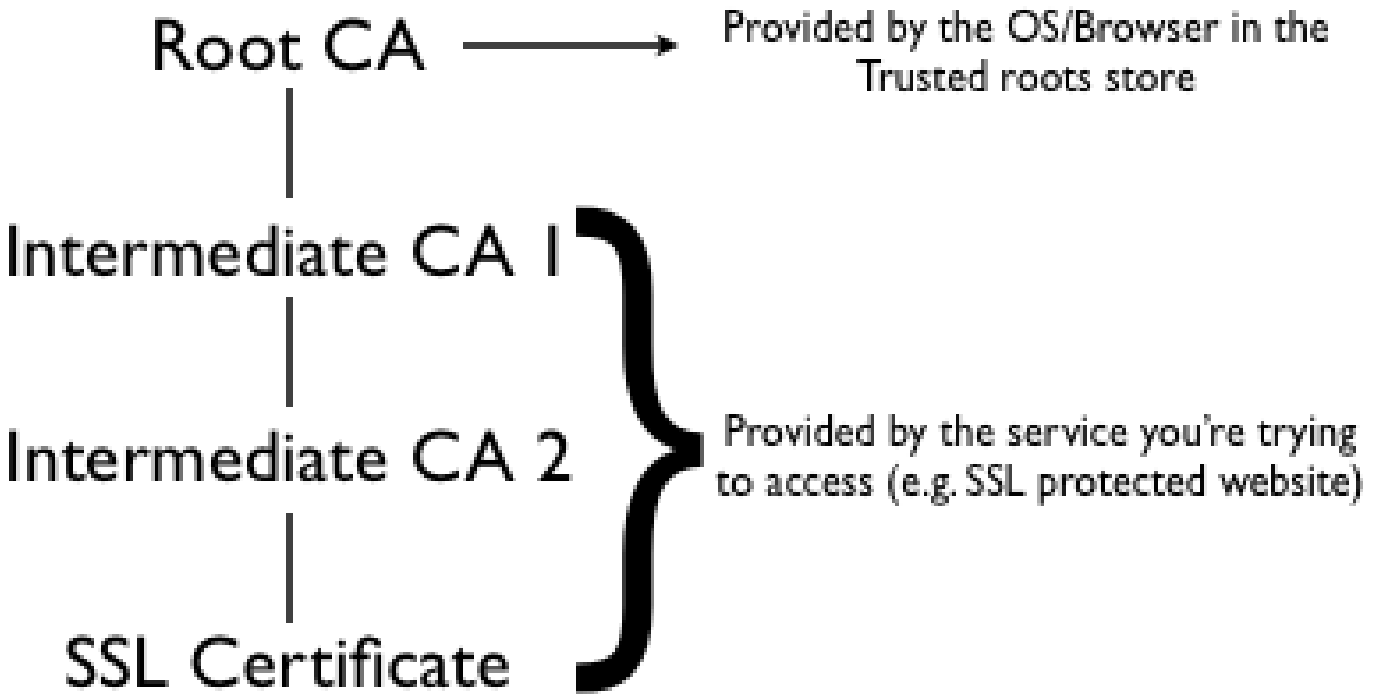
# Содержание

- Некоторые мифы про SSL
- Система CA недостаточно надёжна
- Что предлагает индустрия
- SSL – не “серебрянная пуля”
- Безопасность через управление рисками
- Примеры дополнительных защитных мер

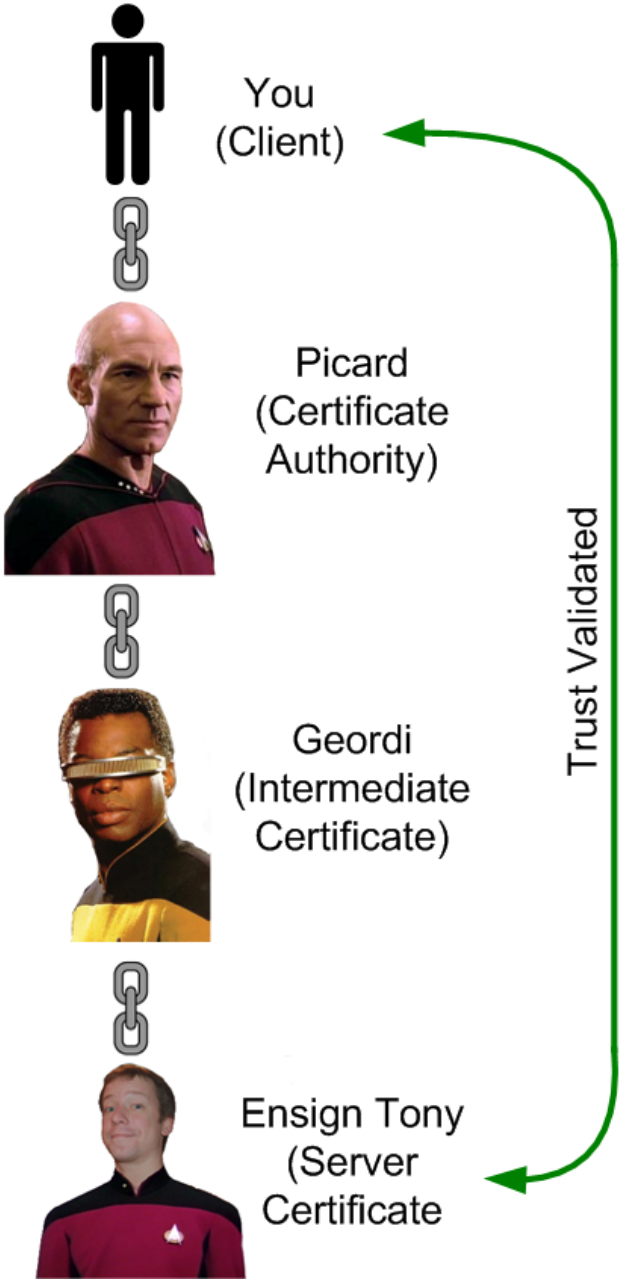
# Благодарность


- Питеру Гутману (Peter Gutmann) за идеи и часть материала

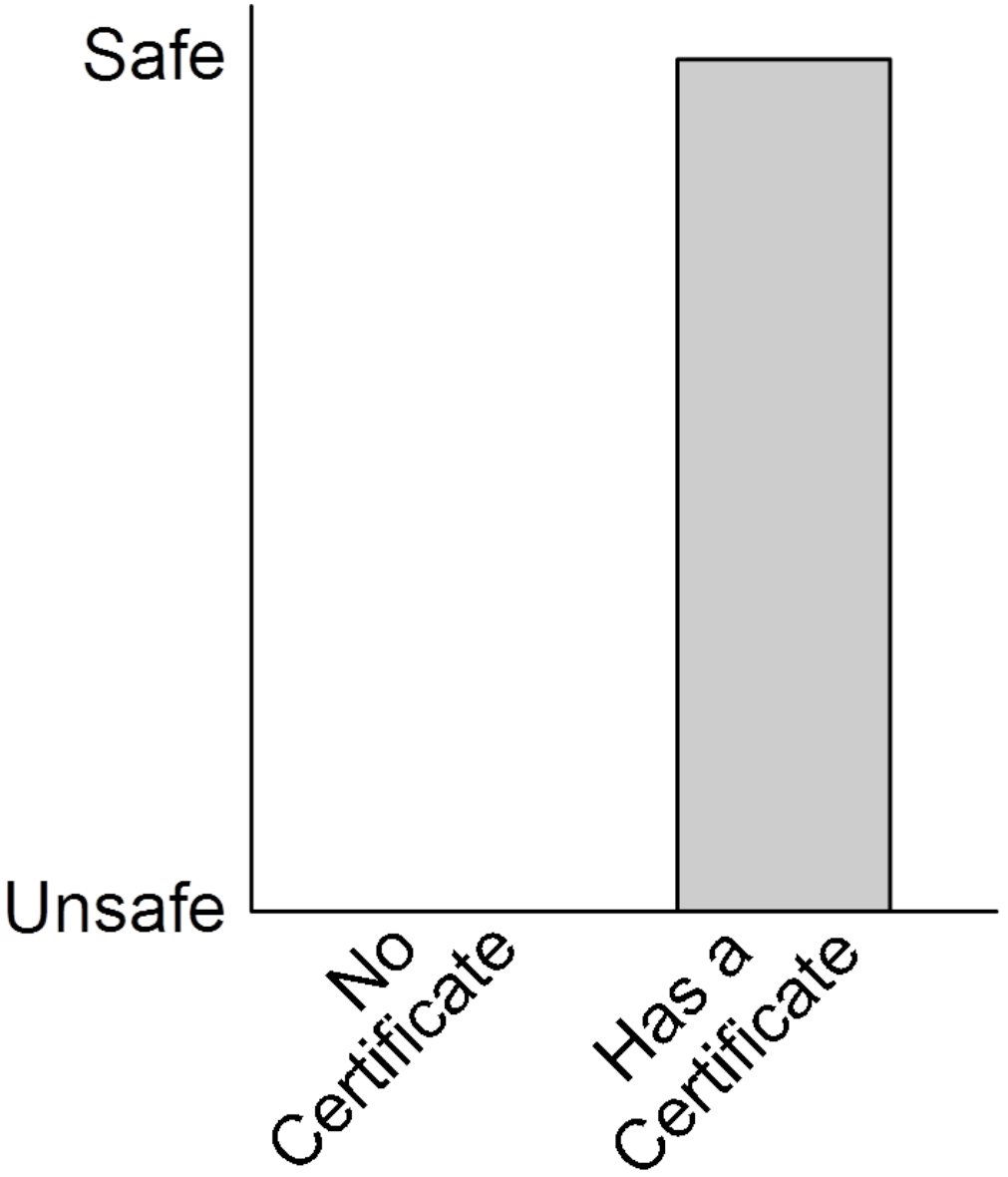
# Безопасность в Web: SSL, CA



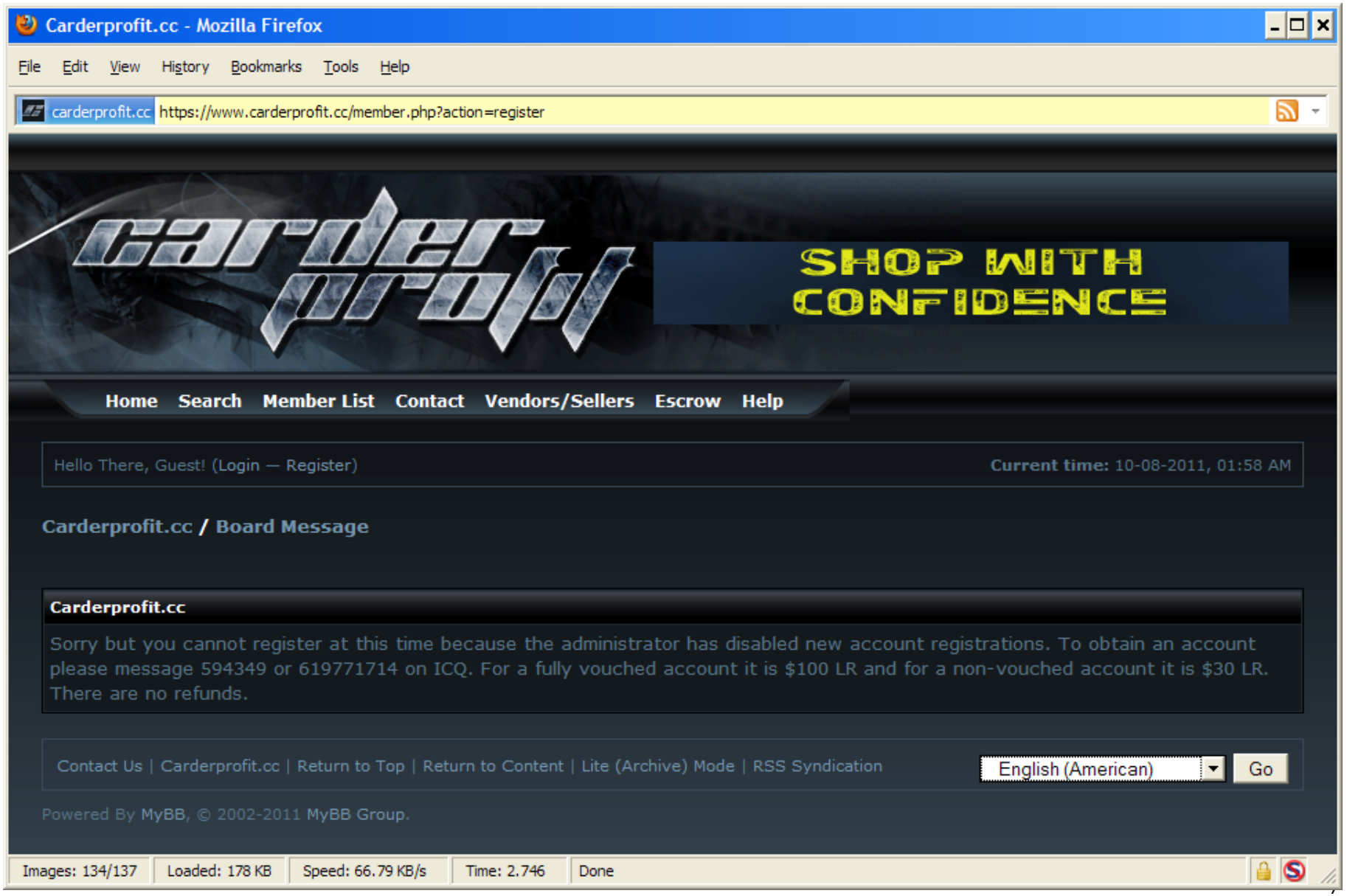
# Безопасность на космических кораблях



# Безопасность в Web: что предполагалось

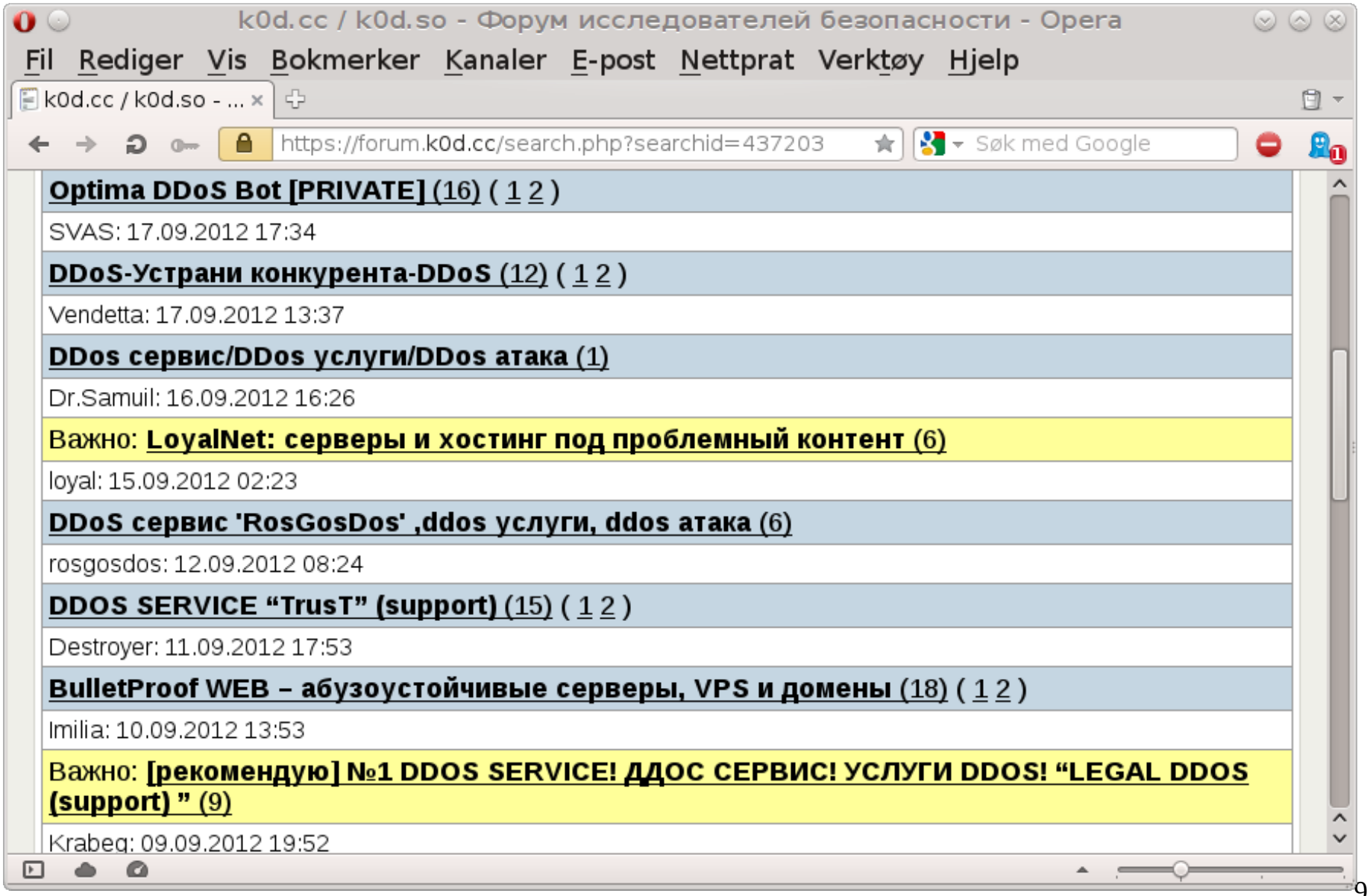


# Сертификат ОК: кардерский сайт, 2011

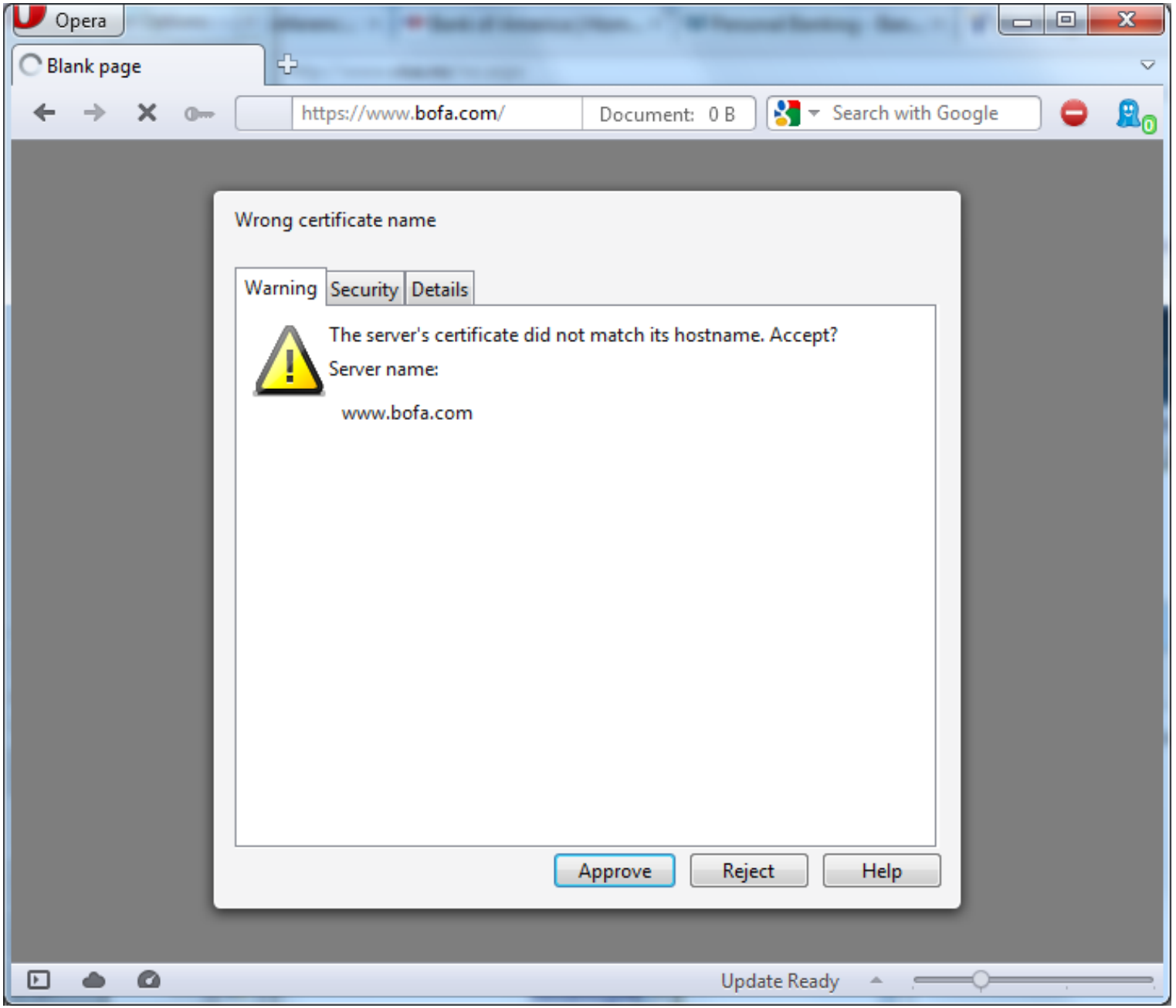


# Тот же сайт, 2012

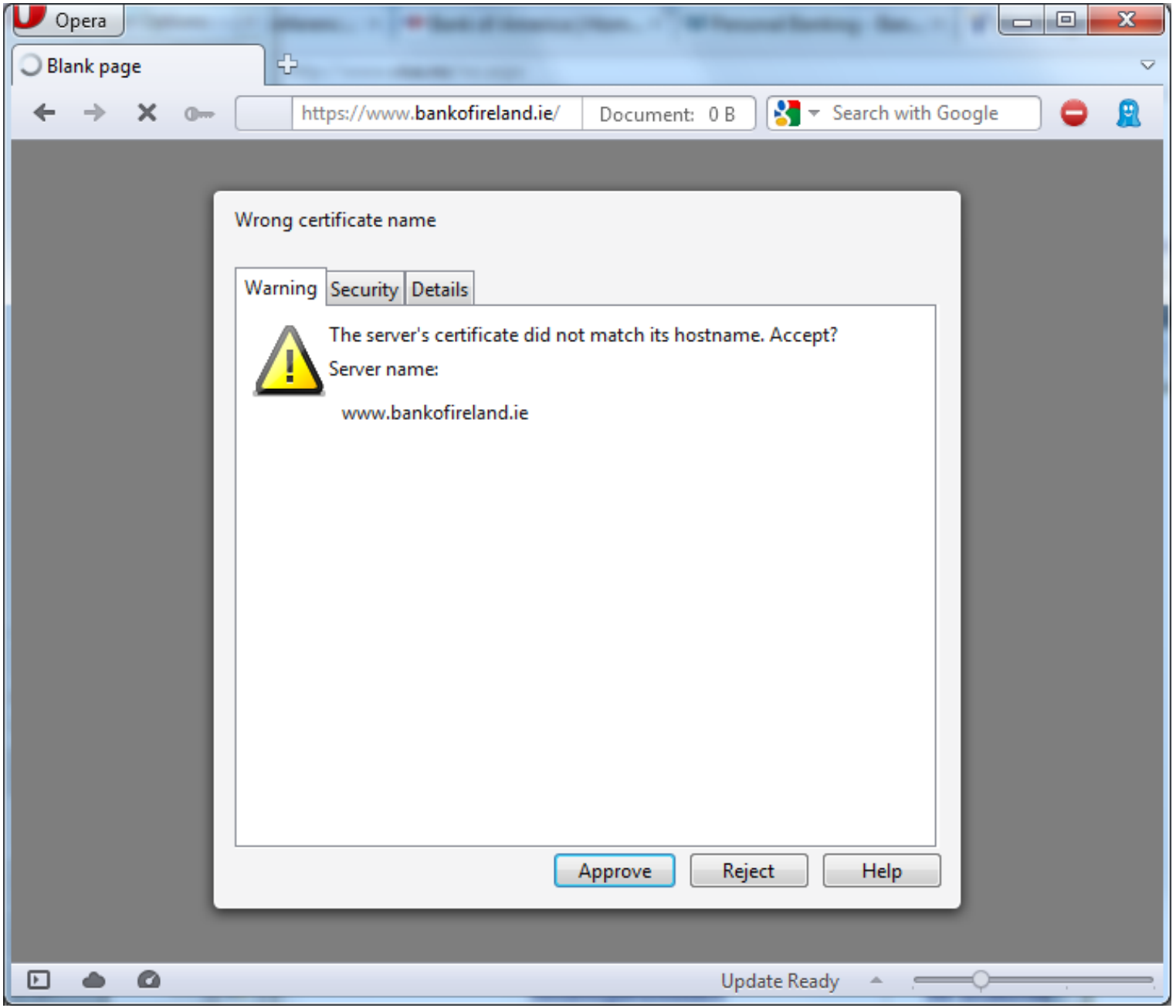
# Сертификат ОК: хакерский форум



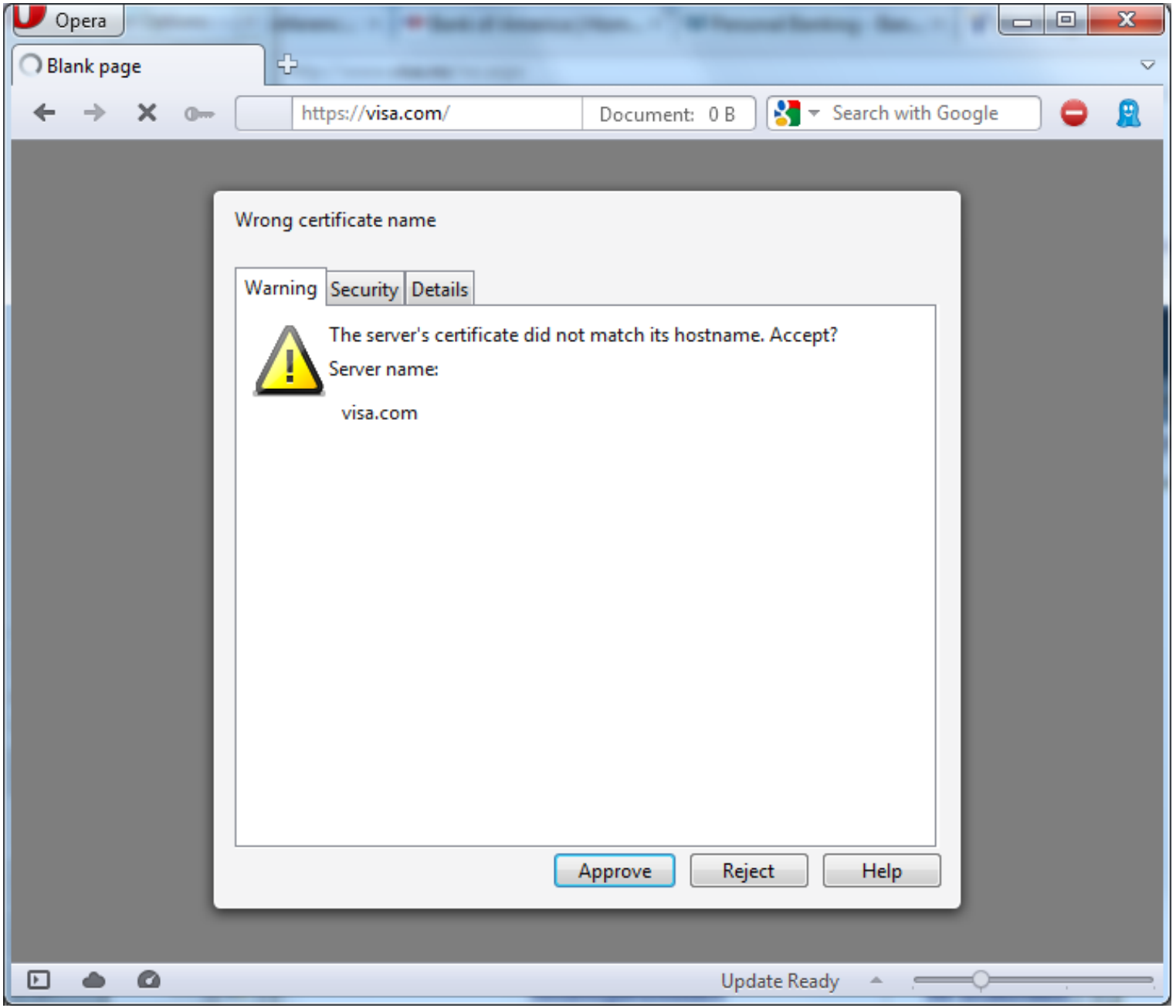
# Сертификат не ОК: Bank of America



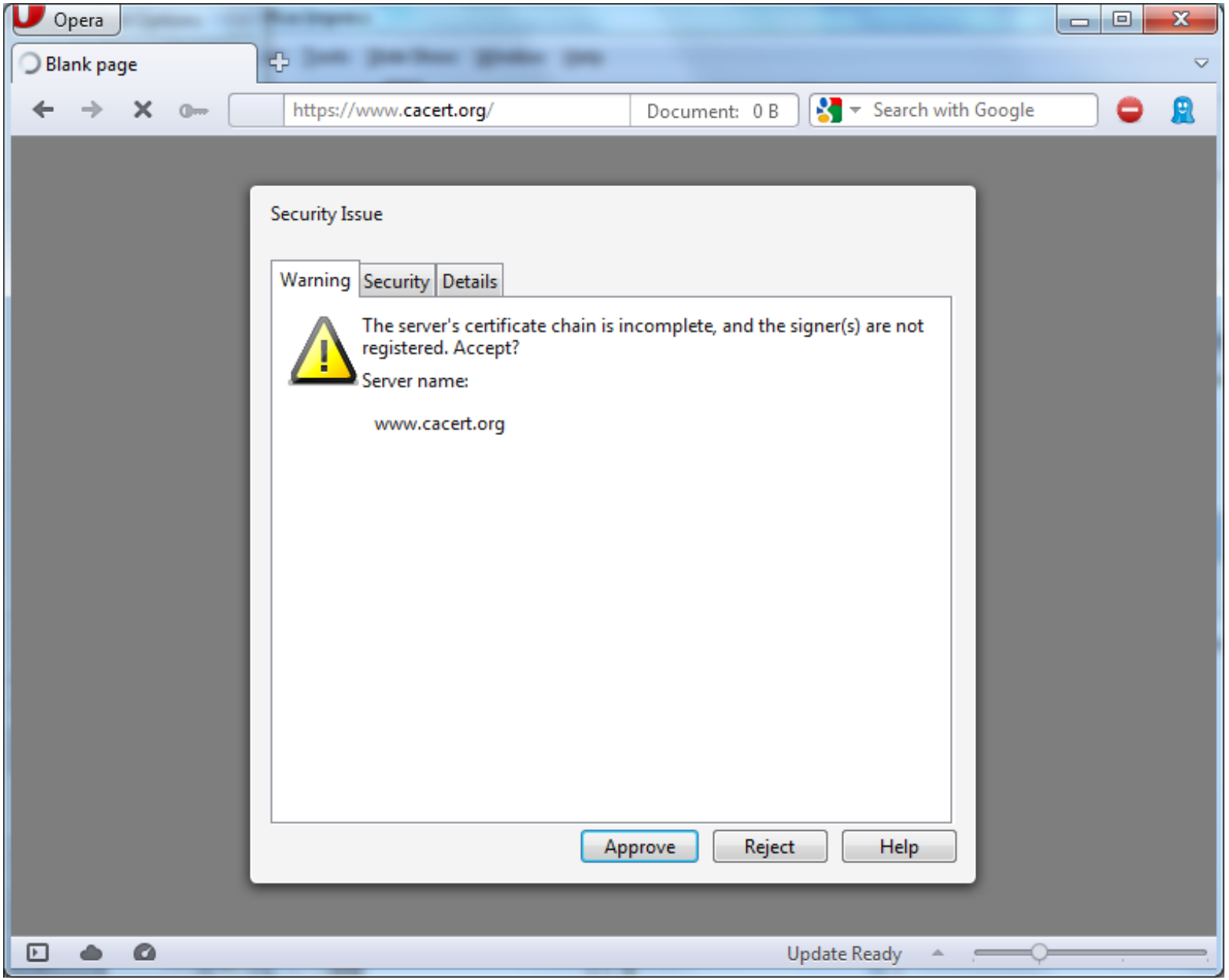
# Сертификат не ОК: Bank of Ireland



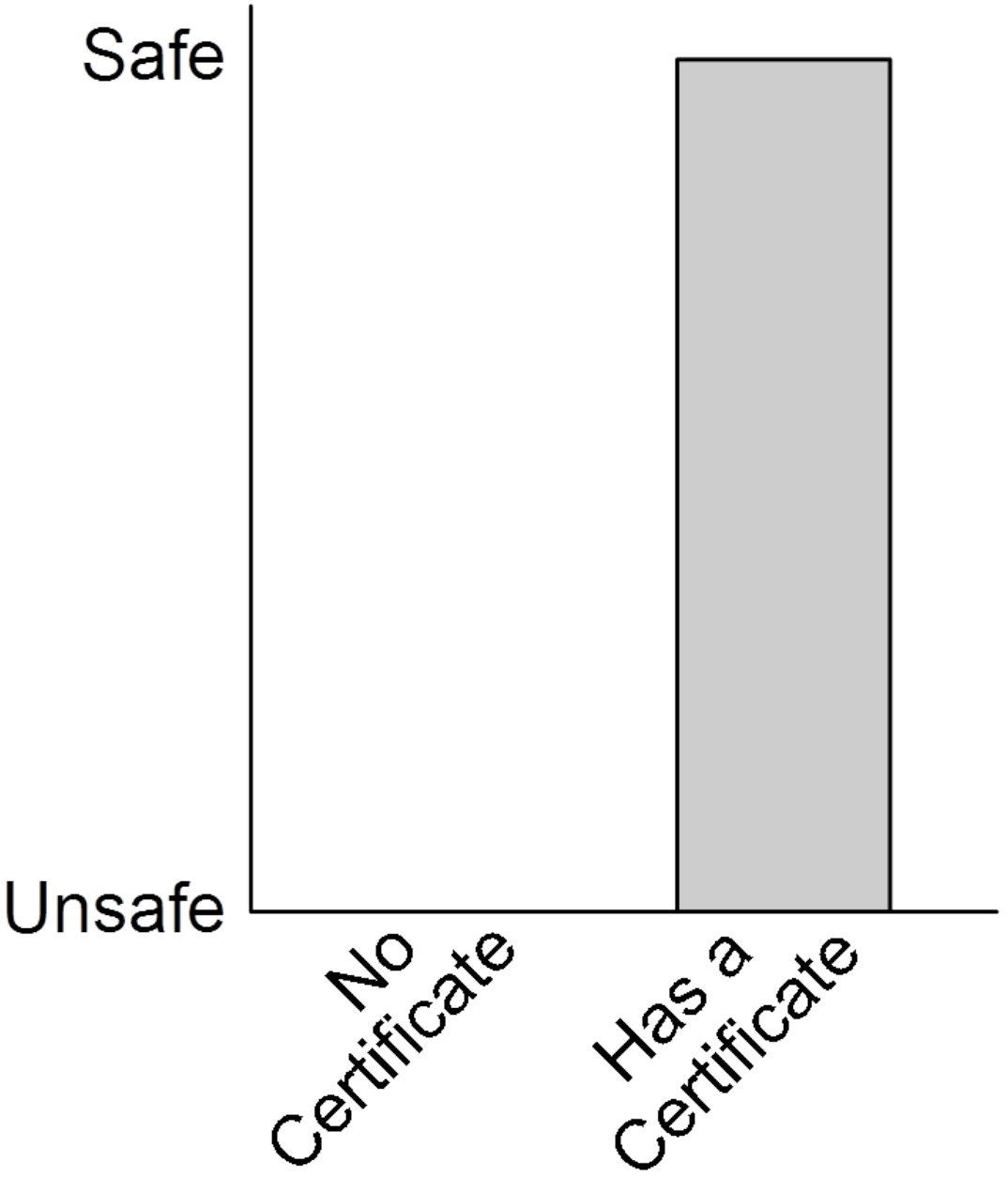
# Сертификат не ОК: VISA



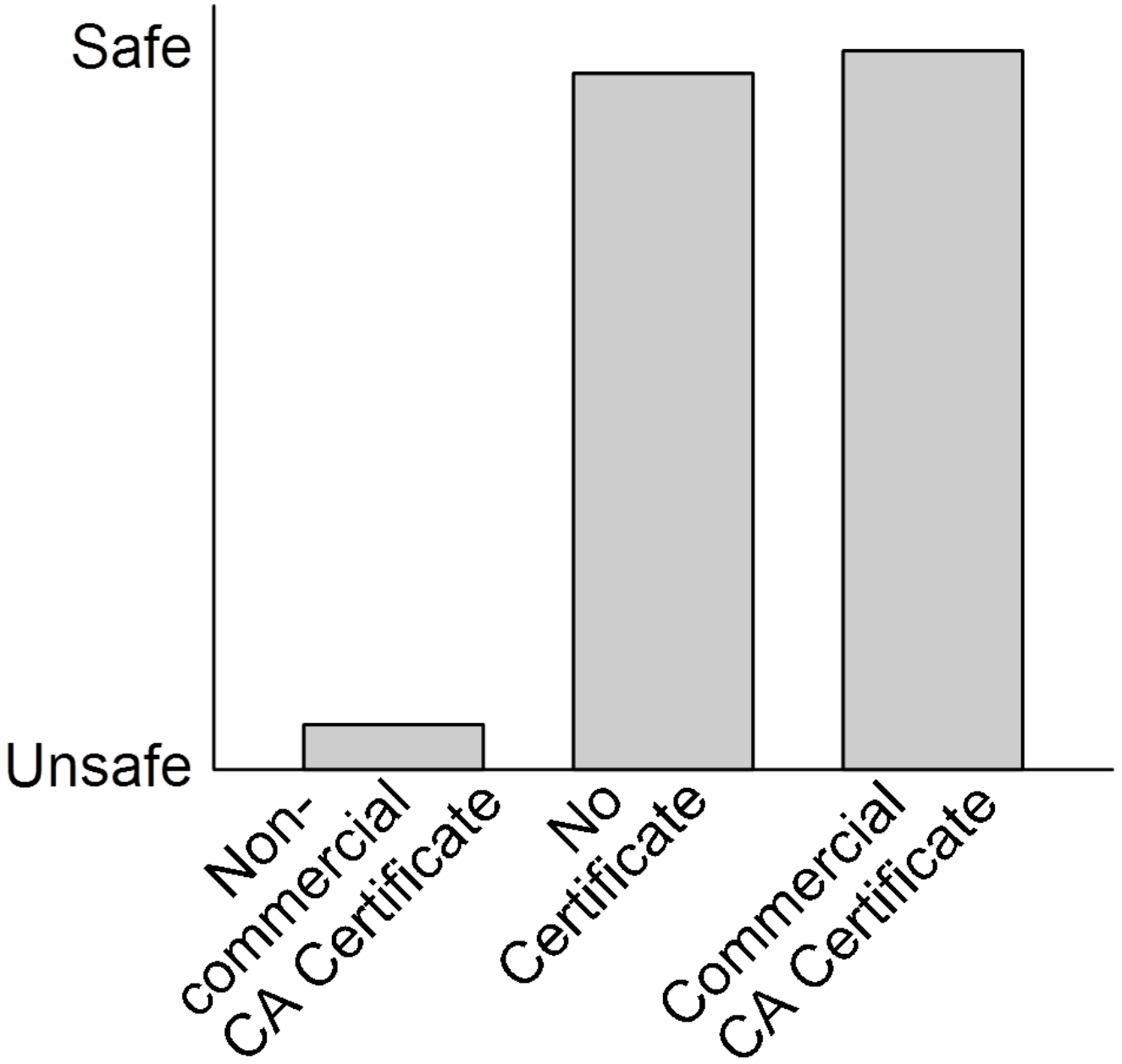
# Некоммерческий CA



# Безопасность в Web: что предполагалось



# Безопасность в Web: что получилось



# Система CA недостаточно надёжна

- Почему мы должны доверять CA?
- Откуда берутся корневые сертификаты у пользователя?

# Система CA недостаточно надёжна

- sslcertificates@live.com

# Система CA недостаточно надёжна

- sslcertificates@live.com
- Взломы CA: Comodo, Diginotar, Verisign

# Система CA недостаточно надёжна

- sslcertificates@live.com
- Взломы CA: Comodo, Diginotar, Verisign
- MITM boxes: Packet Forensics, Cyberoam


Packet Forensics LI-5B

# Чем отвечает индустрия

# Чем отвечает индустрия

- Короткоживущие сертификаты

# Чем отвечает индустрия

- Короткоживущие сертификаты
- OCSP or GTFO

# Чем отвечает индустрия

- Короткоживущие сертификаты
- OCSP or GTFO
- HTTP Strict Transport Security (HSTS)

# Чем отвечает индустрия

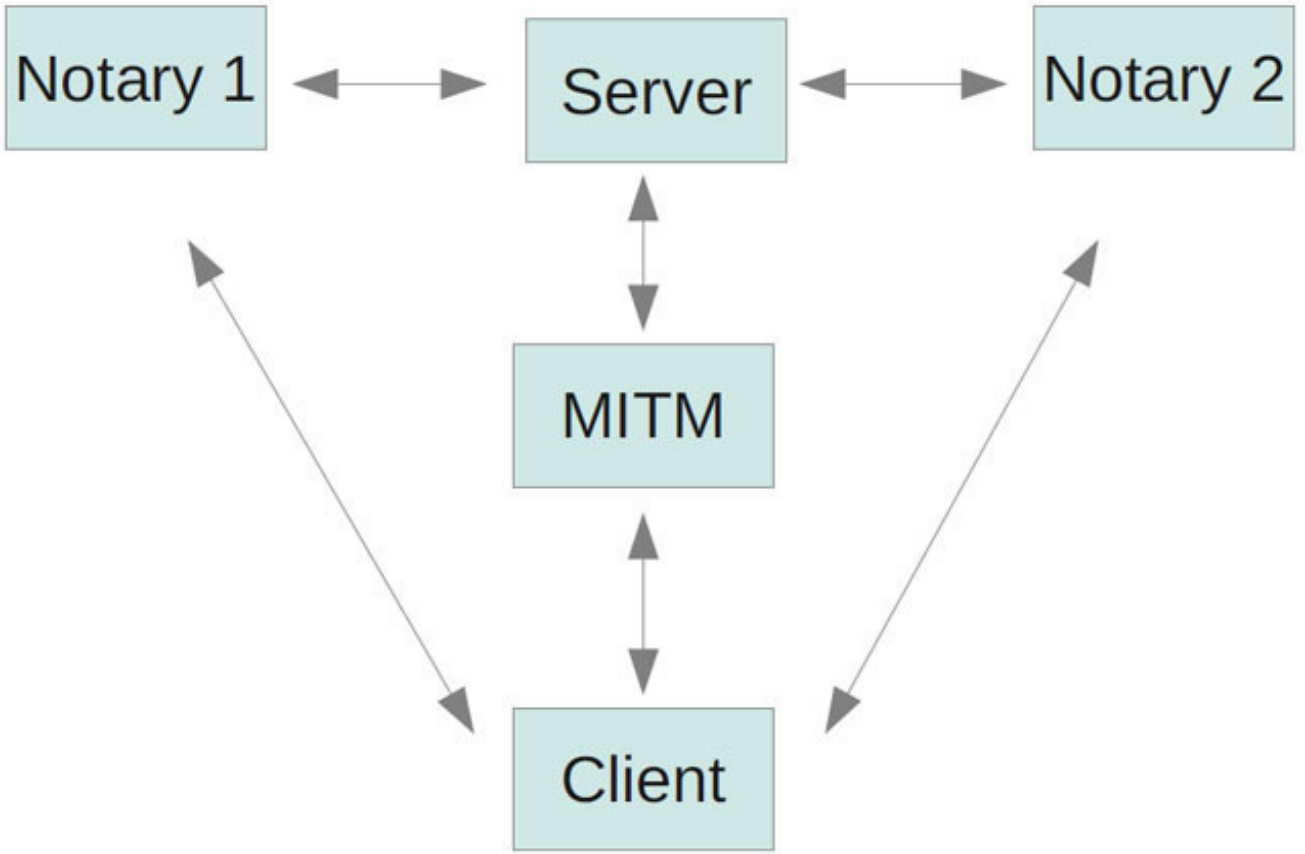
- Короткоживущие сертификаты
- OCSP or GTFO
- HTTP Strict Transport Security (HSTS)
- Certificate logs

# Чем отвечает индустрия

- HTTP Public Key Pinning (HPKP) и TACK

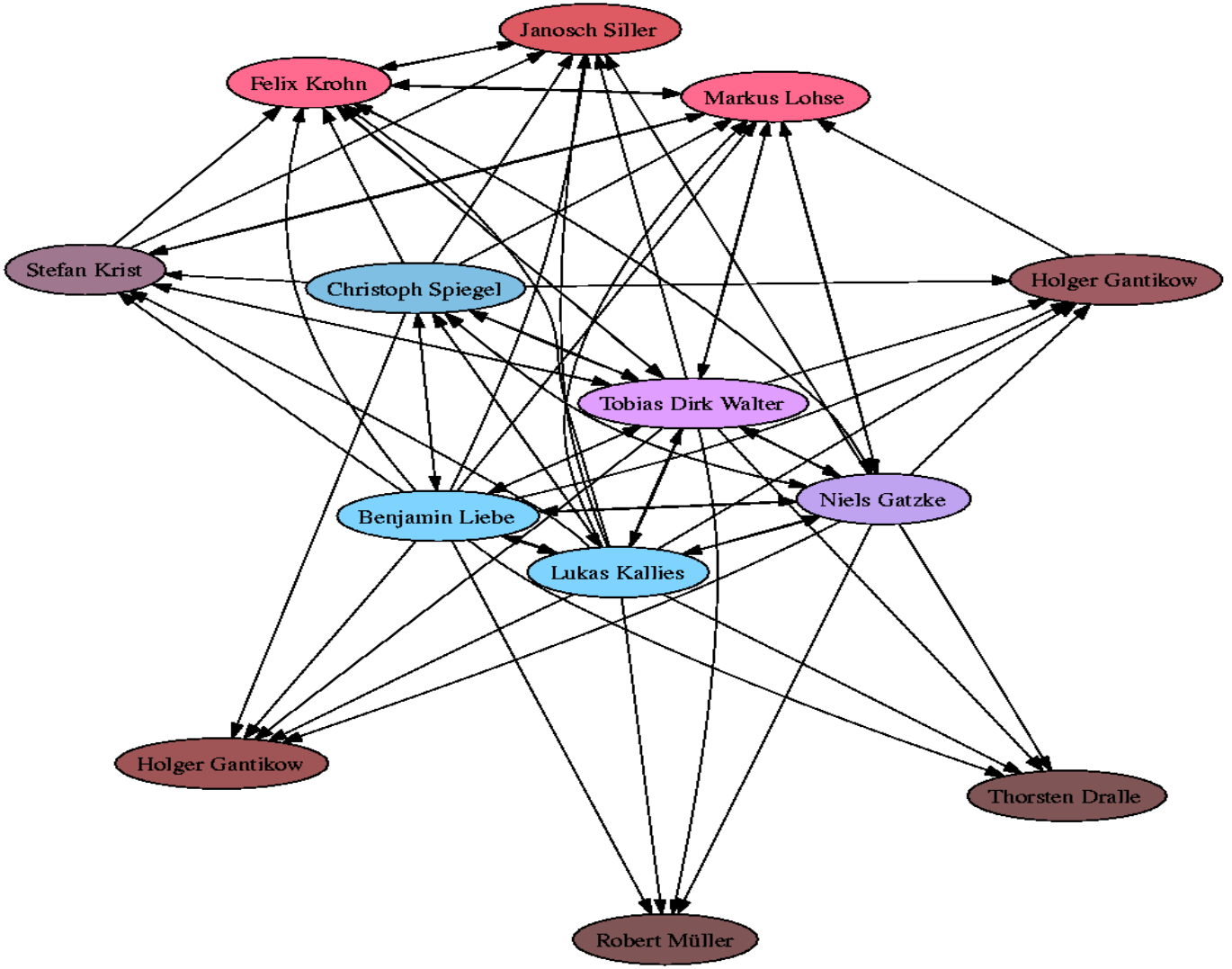
# Чем отвечает индустрия

- Convergence и Mutually Endorsing CA Infr.



# Чем отвечает индустрия

- The Monkeysphere Project и Web of Trust



# PKI them harder

# Молотку всё кажется гвоздём

# PKI – не серебряная пуля

# И уж тем более не священная корова

# Нужна диверсификация защиты

# Диверсификация защиты

- Нет единой точки отказа
- Применяется в реальном мире с начала времён

# Нужна диверсификация защиты

- Что, если механизм защиты отказал?

- Без диверсификации:
  - Отказала вся система
- С диверсификацией:
  - Возрос риск
  - Не отказала вся система

# Безопасность через управление рисками

- Цитата:

  “Управление рисками означает выполнение сознательных действий, направленных на повышение вероятности хорошего исхода дела и уменьшение вероятности плохого исхода дела”

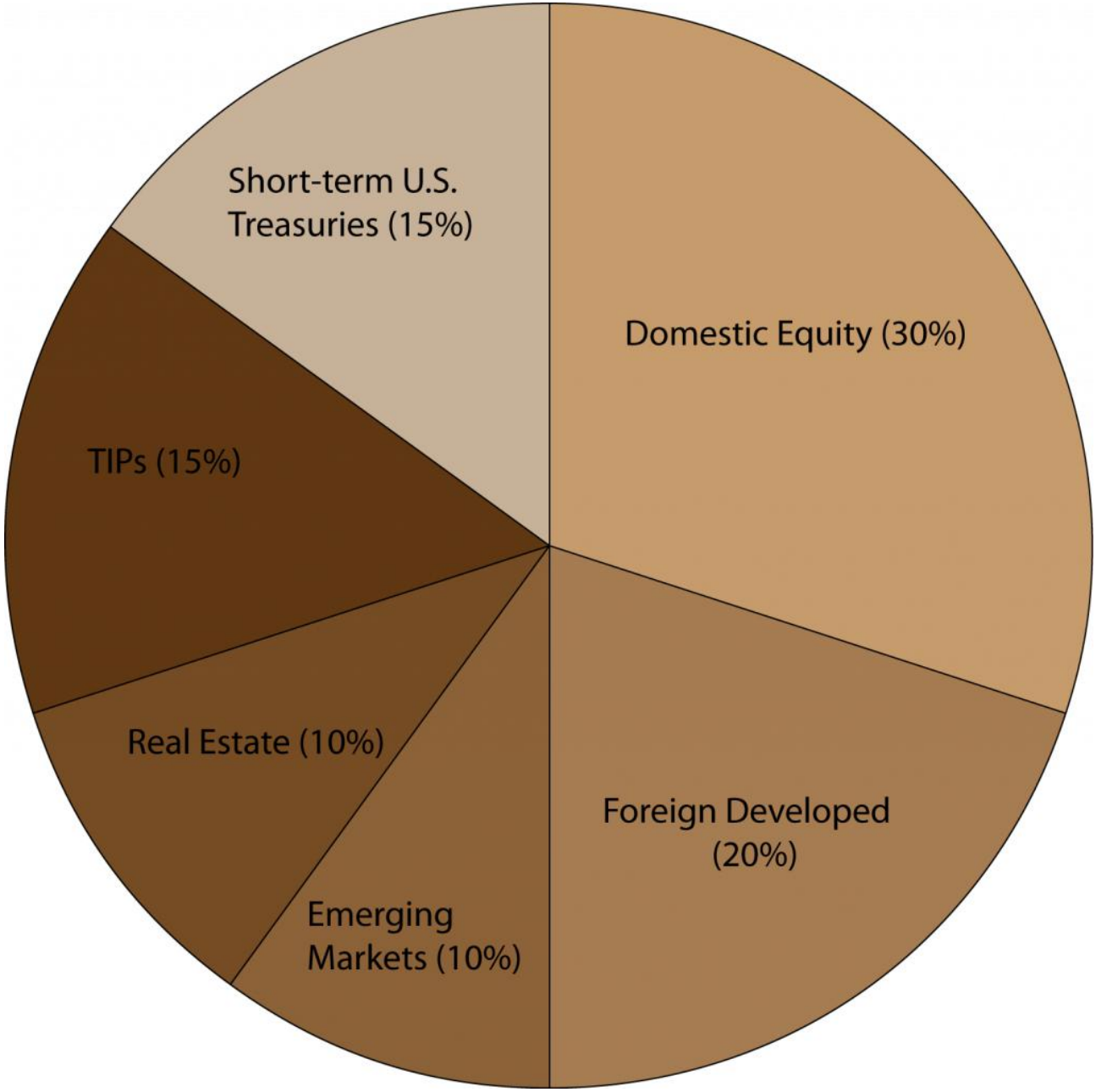
  – Dan Borge, Bankers Trust

# Безопасность через управление рисками

- Комплекс защитных мер
- Ни одна из мер **сама по себе** не даёт сильной защиты
- **Комбинация** простых защитных мер даёт сильную защиту
- Детальная **оценка** безопасности

- Широко используется в экономике
- Применить в Web придумал: Peter Gutmann

# Безопасность через управление рисками



# Не то же самое, что и многоуровневая защита

# Примеры из реального мира

- Парковка в зоне видимости, низкие кусты

# Примеры из реального мира

- Банкомат на виду

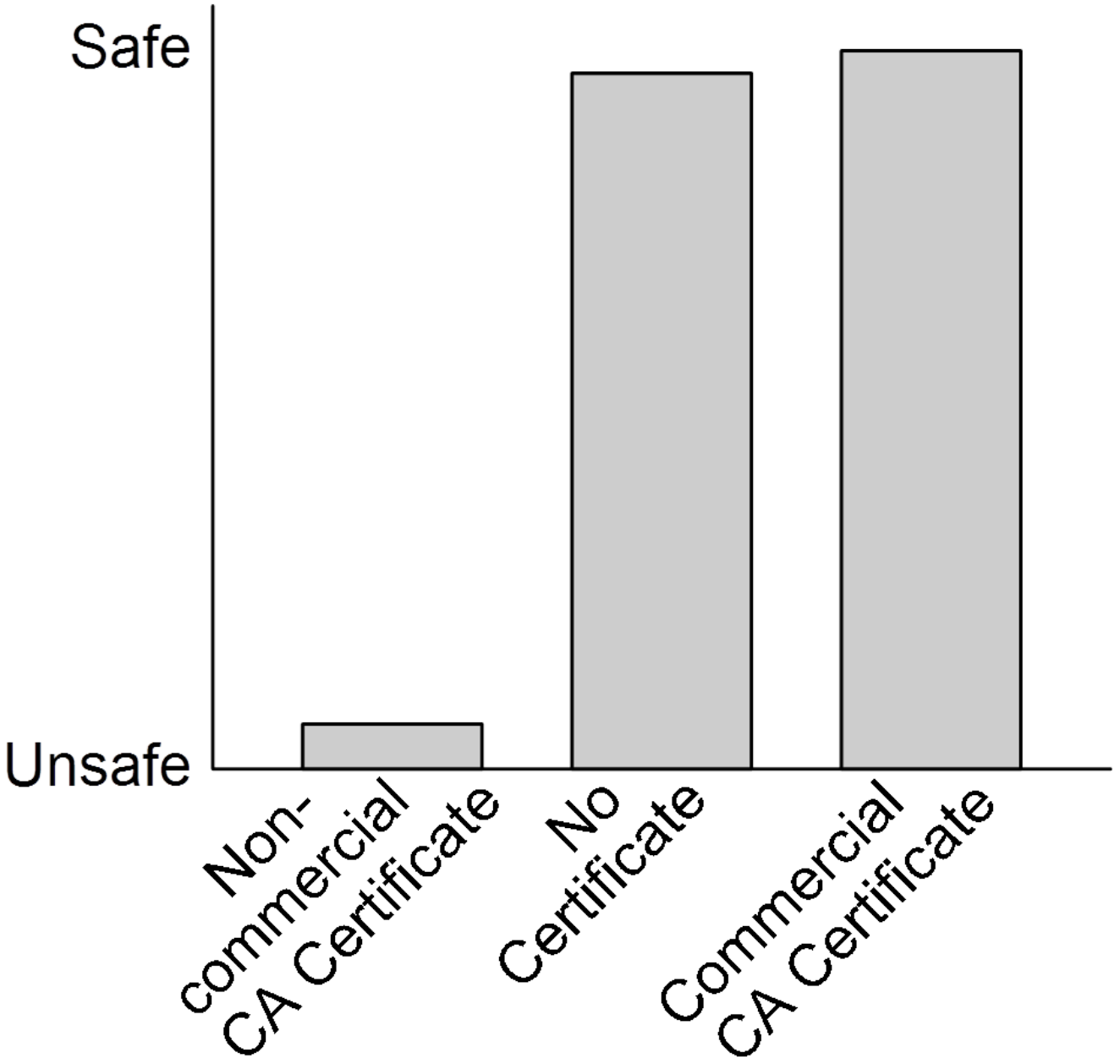
# Примеры из реального мира

- Лианы против граффити

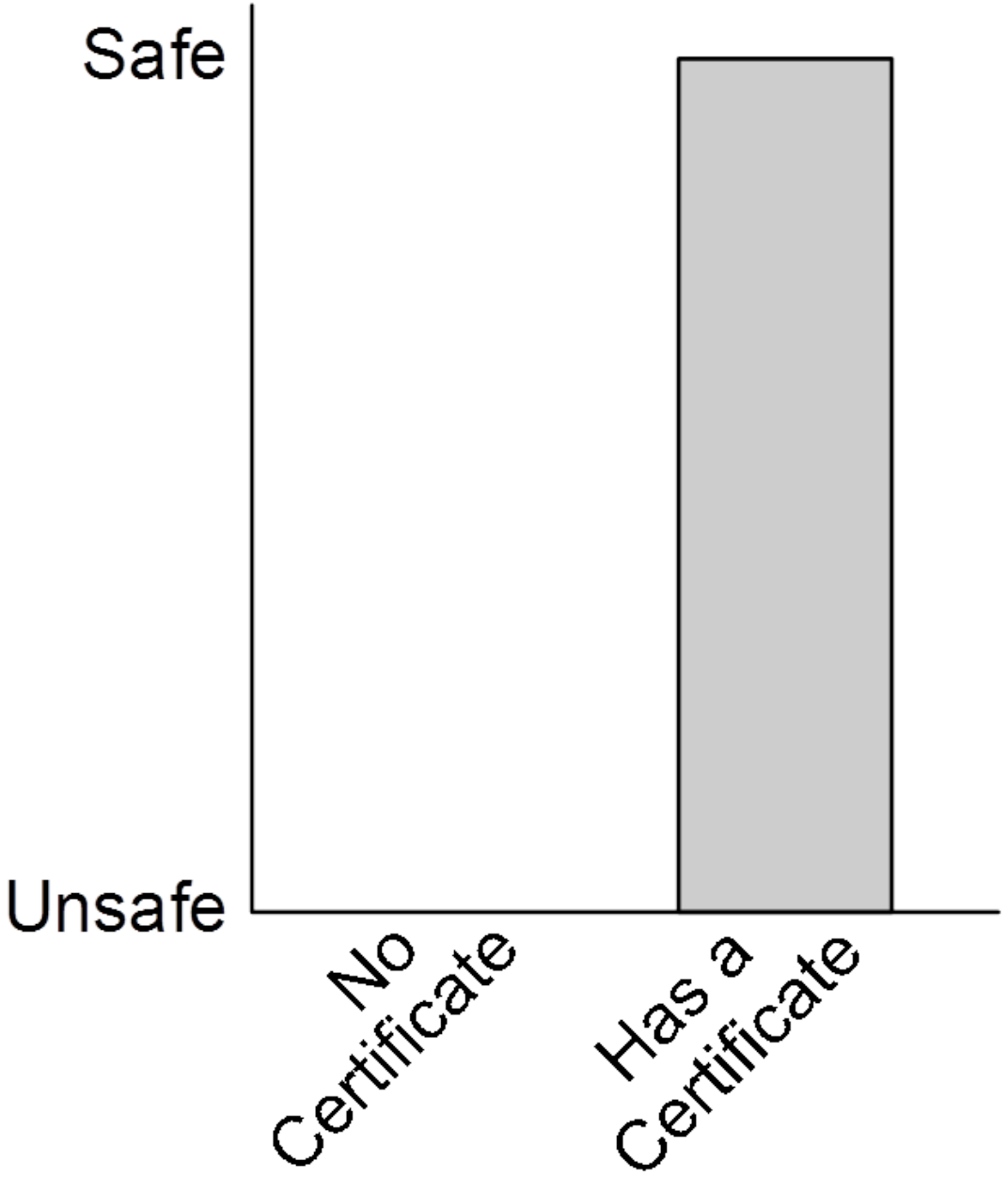
# Безопасность через управление рисками

- Что за ерунда?
  - Парковка перед домом?
  - Лианы?
- Комбинация простых мер даёт в совокупности хорошую защиту

# Текущая ситуация с SSL



# Логичнее было бы так



# Безопасность через управление рисками

- Что за ерунда?
  - А как же цепочка доверия?
  - А как же TACK, Convergence, etc?

- Это вклад в оценку риска.

# Безопасность через управление рисками

- Память в SSL
  - Другой сертификат?
    - И срок действия предыдущего не вышел?
  - Другой ключ?
    - И предыдущий сертификат не отозван?

# Безопасность через управление рисками

- Память в SSL
  - Внезапная смена CA?
    - Французский CA, бразильский сайт?
  - Смена EV на DV?

# Безопасность через управление рисками

- Память в TCP/IP
  - **Кардинально** сменился IP?
    - Совсем другая подсеть?
    - Совсем другая страна?
  - Traceroute стал гораздо короче?

# Безопасность через управление рисками

- Рейтинг CA
  - При текущем “двоичном” подходе невозможен
    - “Замочек” всё равно будет показан
  - Стимулирует экономить на качестве
  - Возможен при управлении рисками

# Безопасность через управление рисками

- История взаимодействия с сайтом

# Безопасность через управление рисками

- История взаимодействия с сайтом

# Безопасность через управление рисками

- Хостинг
  - Whois
  - AS (autonomous system) info

# Безопасность через управление рисками

- Пример: банк Societe Generale
  - Хостится на AS
  - Имя AS: SOCIETE-GENERALE
  - Подключена к французскому бэкбону
  - Работает с 1995 года

# Безопасность через управление рисками

- DNS
  - Reverse lookup: client321.adsl-pool.isp.com
  - Маленький TTL
  - Комбинация записей A, MX, NS
  - Регистратор DNS и IP:
    - RIPE: риск меньше
    - GoDaddy: риск больше

# Безопасность через управление рисками

- TCP/IP stack fingerprint
  - E-commerce сайт хостится на Windows Home Premium?
  - Открыт порт, по которому слушает “популярный” троян?

# Безопасность через управление рисками

- URL
  - Кириллические символы в именах популярных сайтов: yandex.ru
  - Spell-check: panascanic.com, bankoffireland.ie
  - Подстроки: “members”, “adsl-pool”, etc

# Безопасность через управление рисками

- Контент
  - Сравнение с веб-архивом
  - Сравнение с кэшем Google
  - Сравнение с User Agent = Googlebot

# Безопасность через управление рисками

- Контент
  - Страница пытается задействовать известные уязвимости?
  - HTML тэги в “неправильных” местах?
  - Несколько тэгов html, head, title, body?
  - Много объектов подгружается из других доменов?
    - См. проверку URL

# Безопасность через управление рисками

- Javascript
  - Длинные строки и их энтропия
  - Вызовы eval(), большое количество substring(), concat(), fromCharCode()

# Безопасность через управление рисками

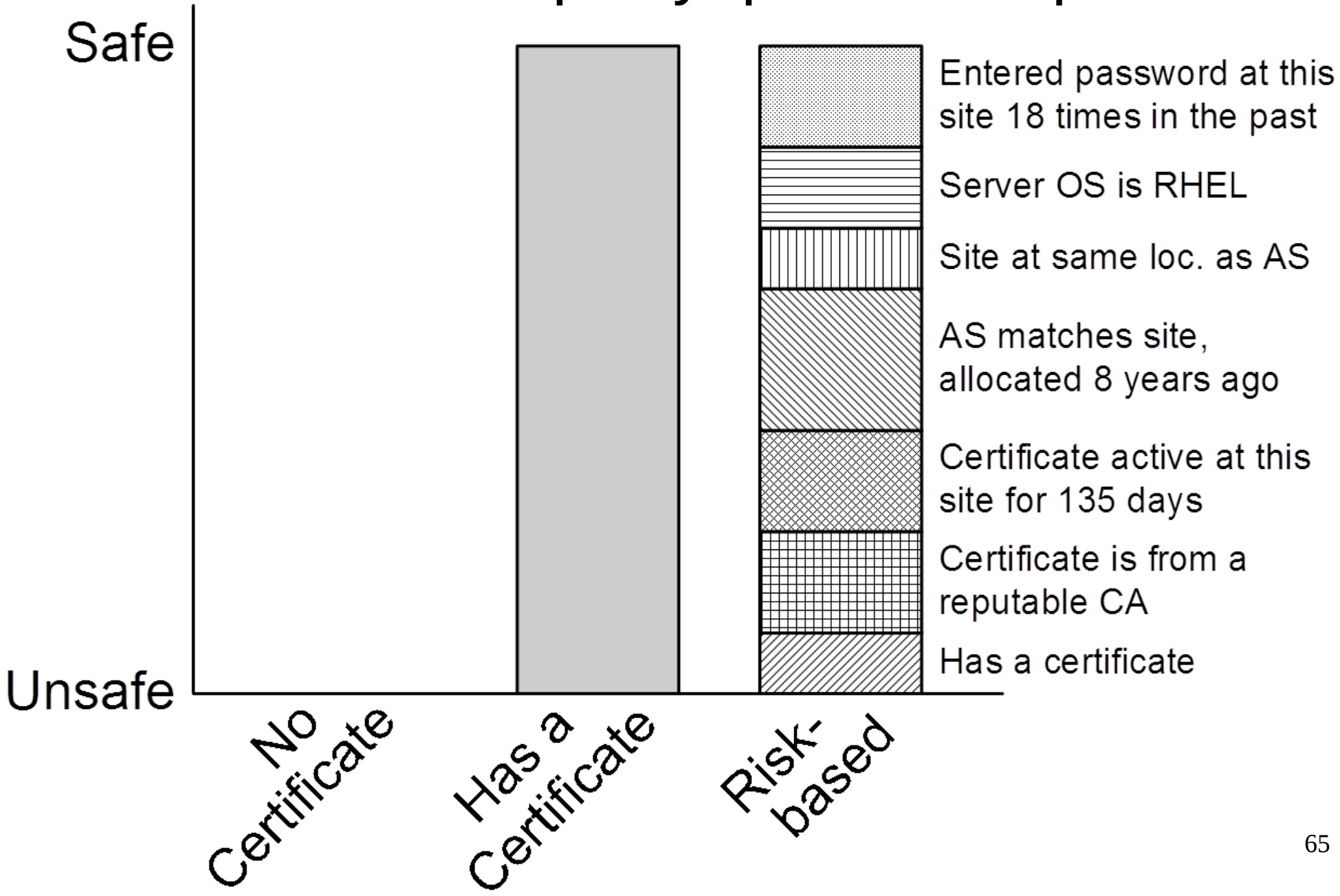
- Байесовский фильтр

Reverend Thomas Bayes

# Безопасность через управление рисками

- Обфускация контента
  - Несложно
  - Но вызывает подозрение
  - Механизмы анти-детектирования сами облегчают детектирование

# Безопасность через управление рисками



# Но ведь...

- Это же скажется на производительности!
  - Не все сайты надо проверять тщательно
  - Оптимизация
    - Проверки одновременно с загрузкой страницы
    - Кэширование результатов
    - Префетчинг

# Выводы

- Браузерам есть куда расти
  - PKI недостаточно надёжно, и оно не везде
  - Чёрные списки работают плохо
- Надо применять управление рисками
  - Проверено временем в реальном мире
  - Можно использовать и в Web

# Спасибо за внимание!

Вопросы?