

# Безопасность в браузерах: Альтернативы SSL

Алексей Хлебников

LVEE 2017

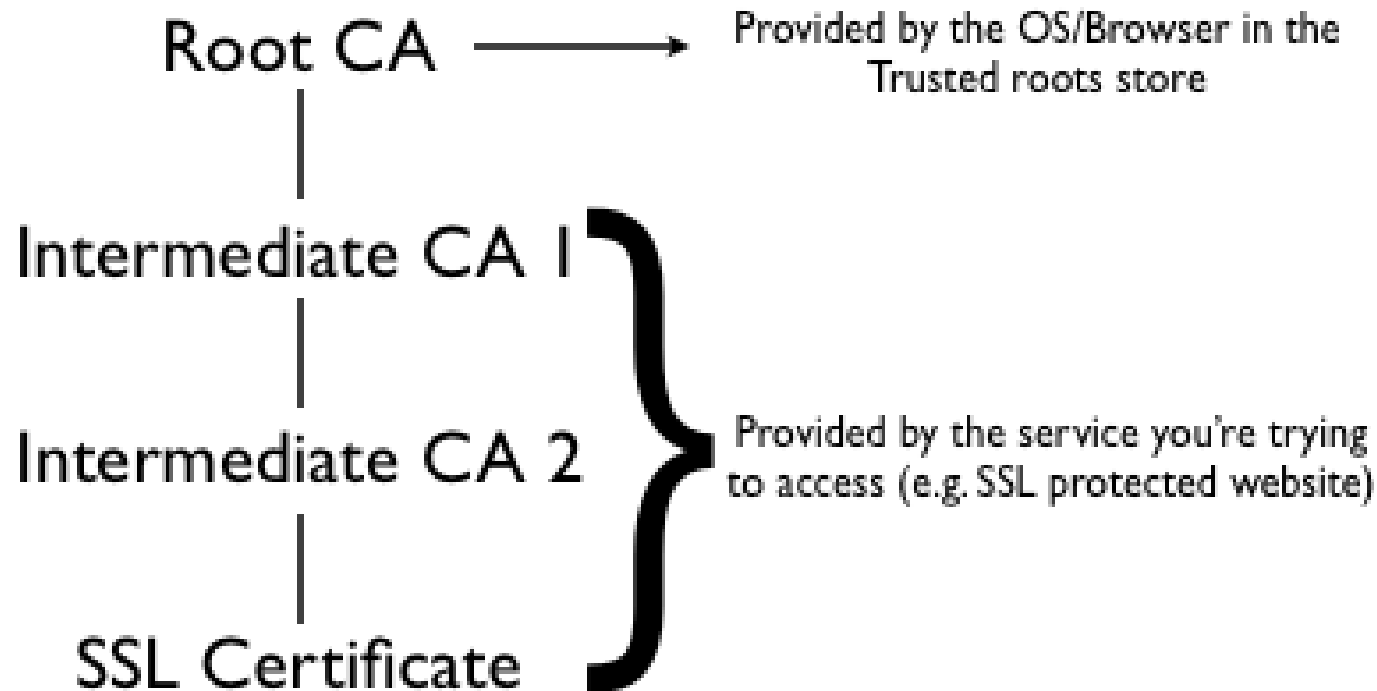
# Содержание

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

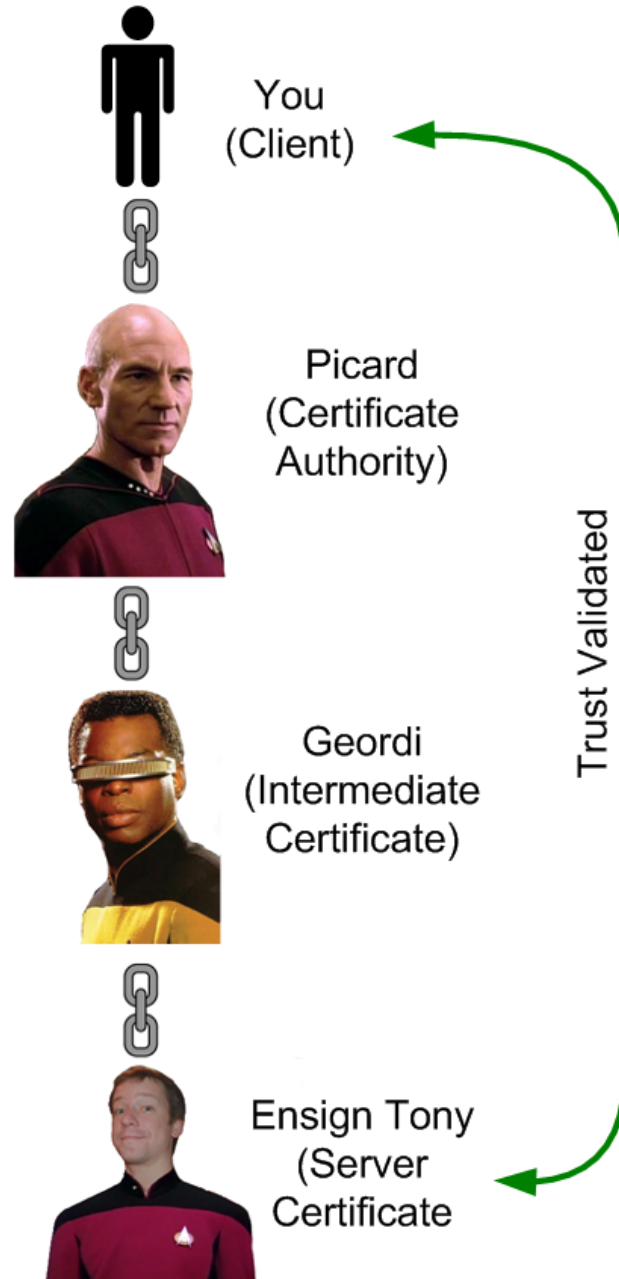
# Благодарность

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

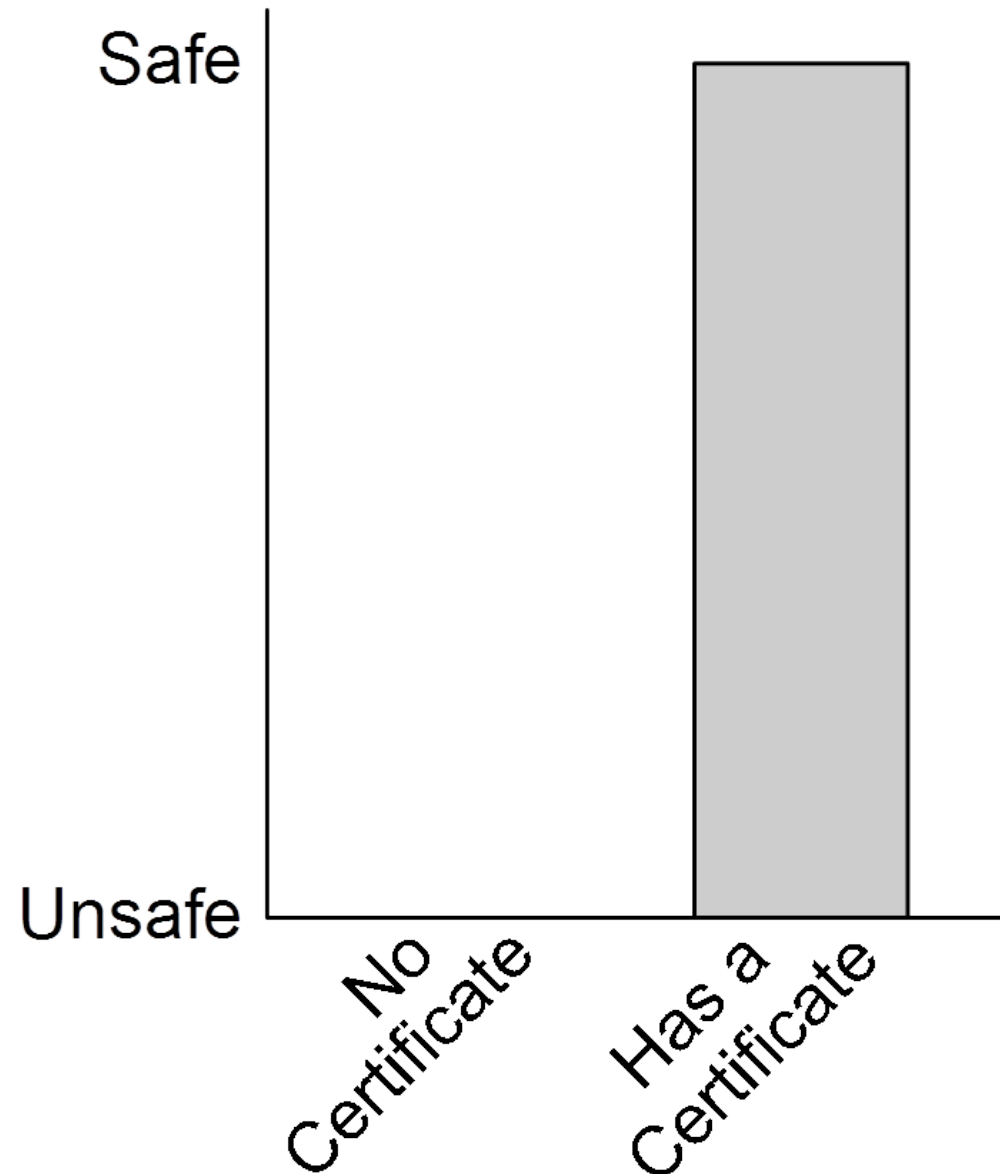
# Безопасность в Web: SSL, CA



# Безопасность на космических кораблях



# Безопасность в Web: что предполагалось



# Сертификат ОК: кардерский сайт, 2011

Carderprofit.cc - Mozilla Firefox

File Edit View History Bookmarks Tools Help

carderprofit.cc https://www.carderprofit.cc/member.php?action=register

# Carder Profit

**SHOP WITH CONFIDENCE**

[Home](#) [Search](#) [Member List](#) [Contact](#) [Vendors/Sellers](#) [Escrow](#) [Help](#)

Hello There, Guest! ([Login](#) — [Register](#)) Current time: 10-08-2011, 01:58 AM

## Carderprofit.cc / Board Message

**Carderprofit.cc**

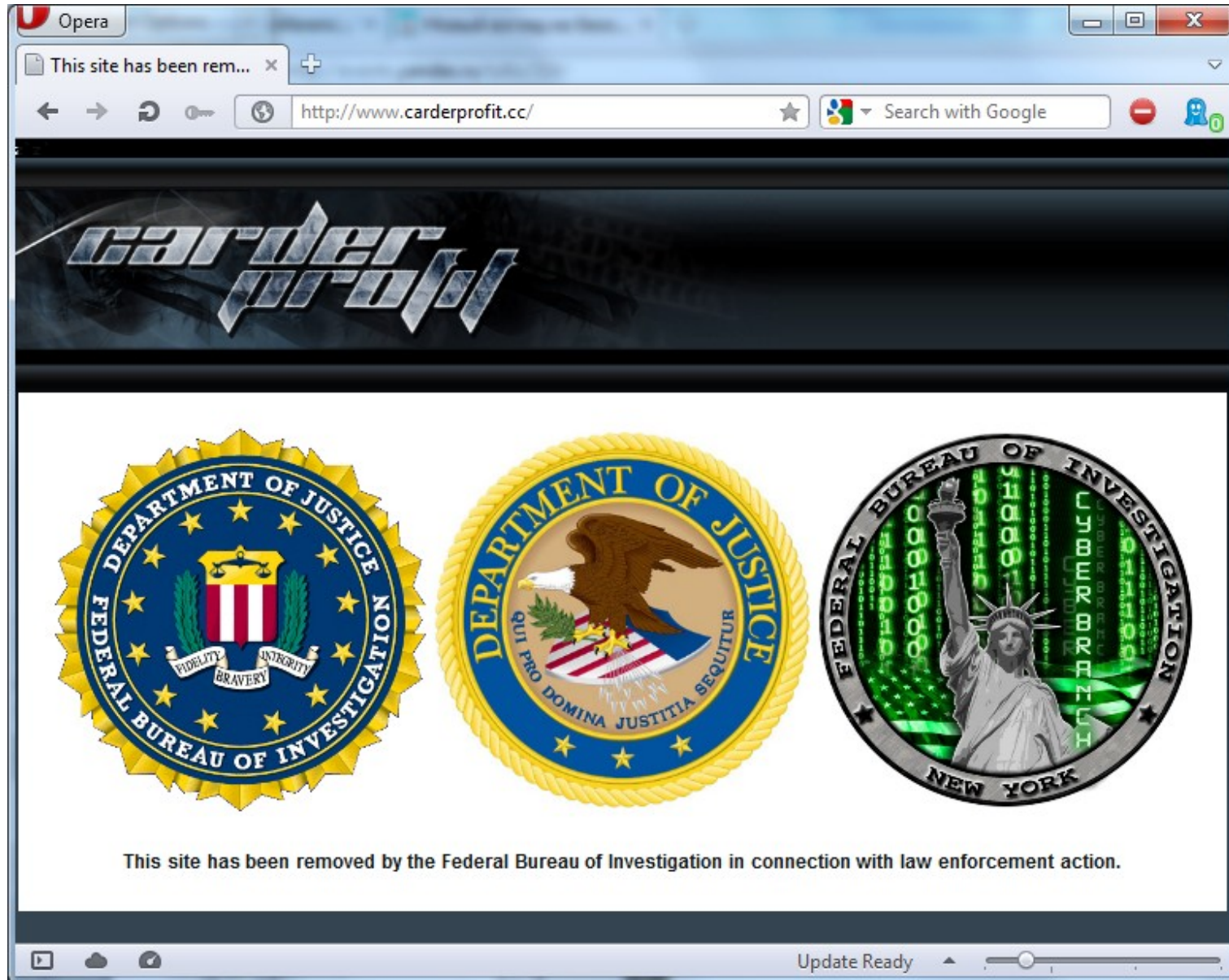
Sorry but you cannot register at this time because the administrator has disabled new account registrations. To obtain an account please message 594349 or 619771714 on ICQ. For a fully vouched account it is \$100 LR and for a non-vouched account it is \$30 LR. There are no refunds.

[Contact Us](#) | [Carderprofit.cc](#) | [Return to Top](#) | [Return to Content](#) | [Lite \(Archive\) Mode](#) | [RSS Syndication](#) English (American)

Powered By MyBB, © 2002-2011 MyBB Group.

Images: 134/137   Loaded: 178 KB   Speed: 66.79 KB/s   Time: 2.746   Done

# Тот же сайт, 2012



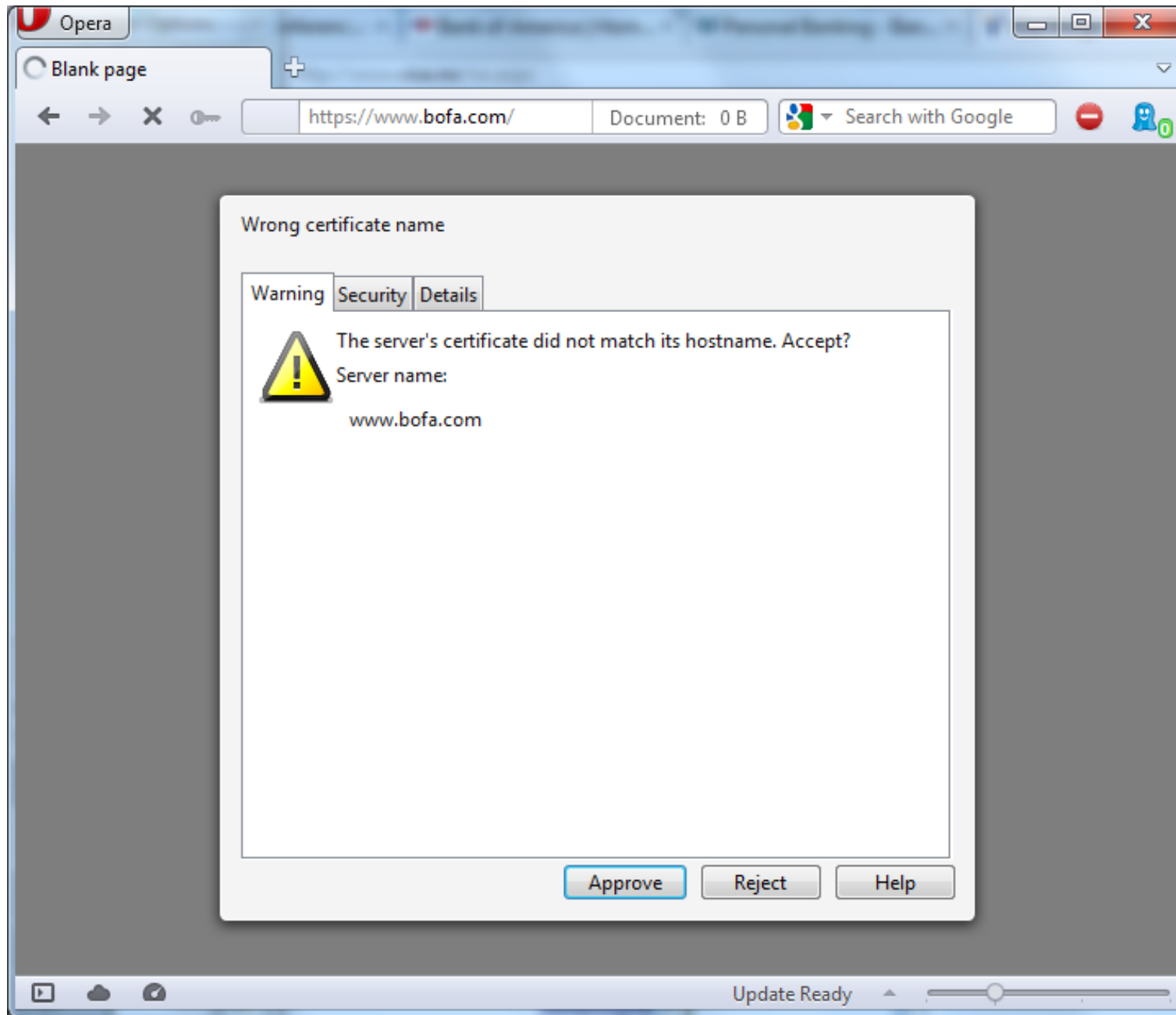


# Сертификат ОК: хакерский форум

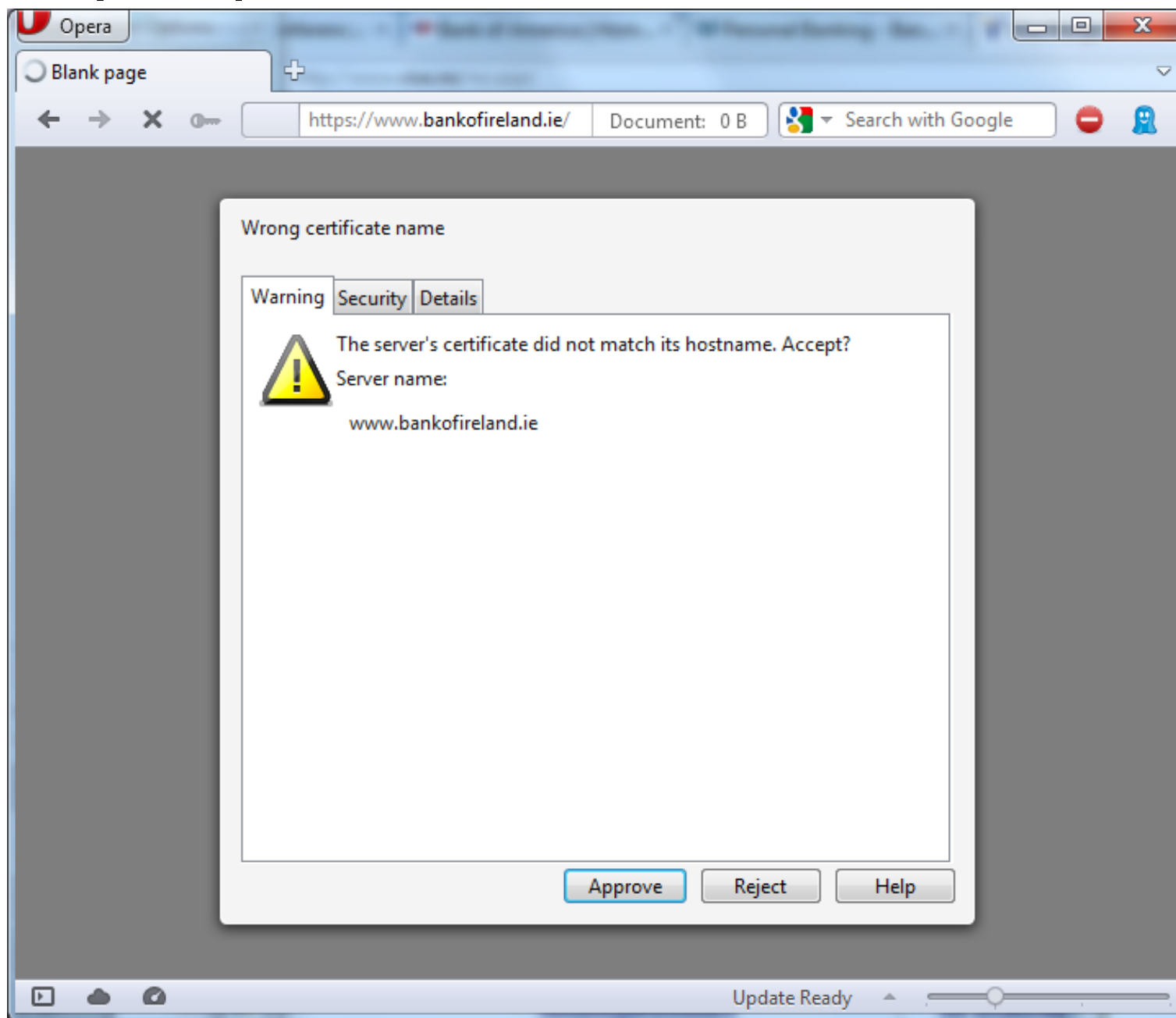
Opera browser window showing a search results page on the forum k0d.cc / k0d.so. The search query is "https://forum.k0d.cc/search.php?searchid=437203". The results list several threads related to DDoS attacks and services.

Thread Title	Author	Date
<b>Optima DDoS Bot [PRIVATE] (16) ( 1 2 )</b>	SVAS	17.09.2012 17:34
<b>DDoS-Устрани конкурента-DDoS (12) ( 1 2 )</b>	Vendetta	17.09.2012 13:37
<b>DDos сервис/DDos услуги/DDos атака (1)</b>	Dr.Samuil	16.09.2012 16:26
<b>Важно: LoyalNet: серверы и хостинг под проблемный контент (6)</b>	loyal	15.09.2012 02:23
<b>DDoS сервис 'RosGosDos' ,ddos услуги, ddos атака (6)</b>	rosgosdos	12.09.2012 08:24
<b>DDOS SERVICE "Trust" (support) (15) ( 1 2 )</b>	Destroyer	11.09.2012 17:53
<b>BulletProof WEB - abusoустойчивые серверы, VPS и домены (18) ( 1 2 )</b>	Imilia	10.09.2012 13:53
<b>Важно: [рекомендую] №1 DDOS SERVICE! ДДОС СЕРВИС! УСЛУГИ DDOS! "LEGAL DDOS (support)" (9)</b>	Krabeq	09.09.2012 19:52

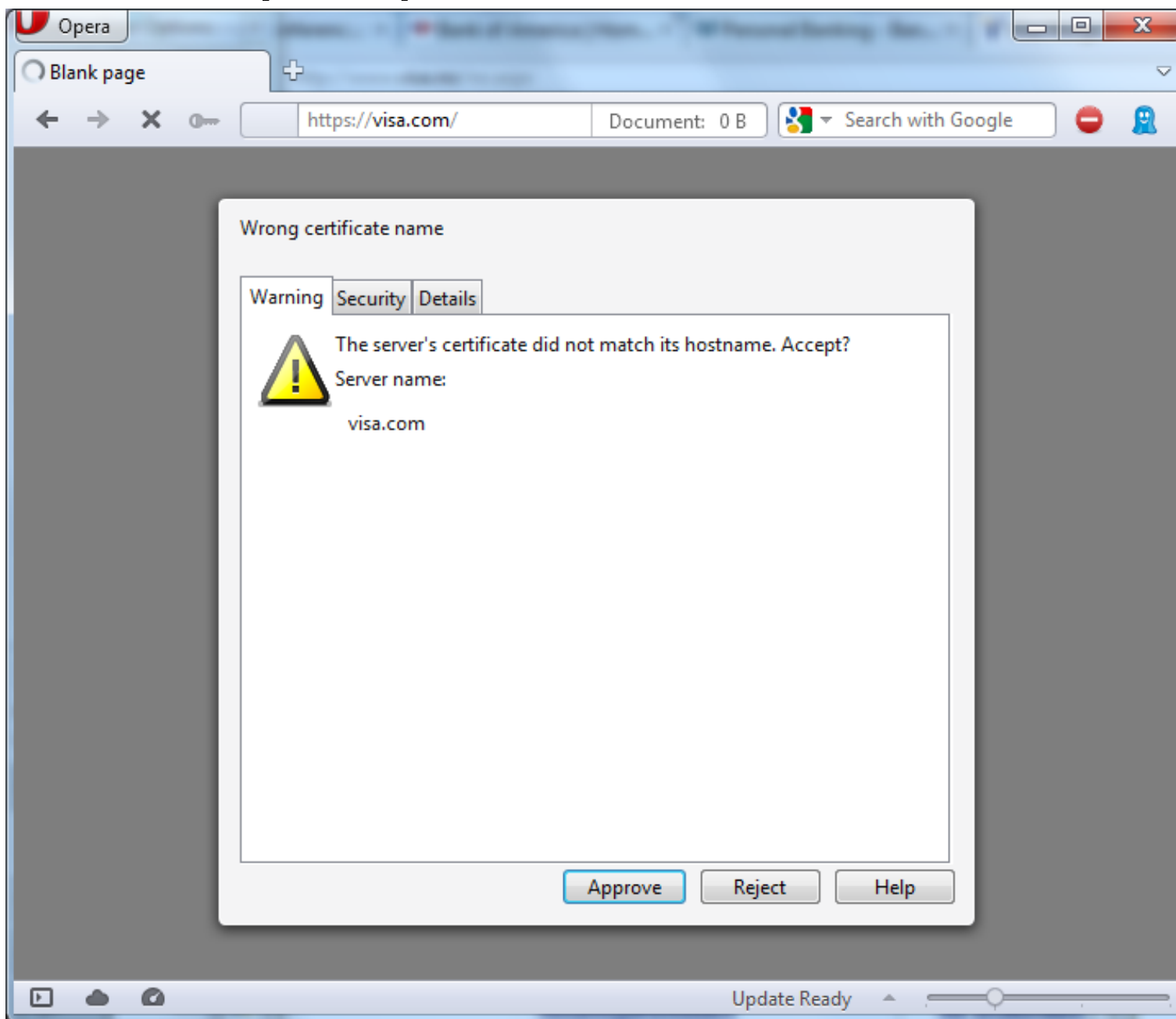
# Сертификат не ОК: Bank of America



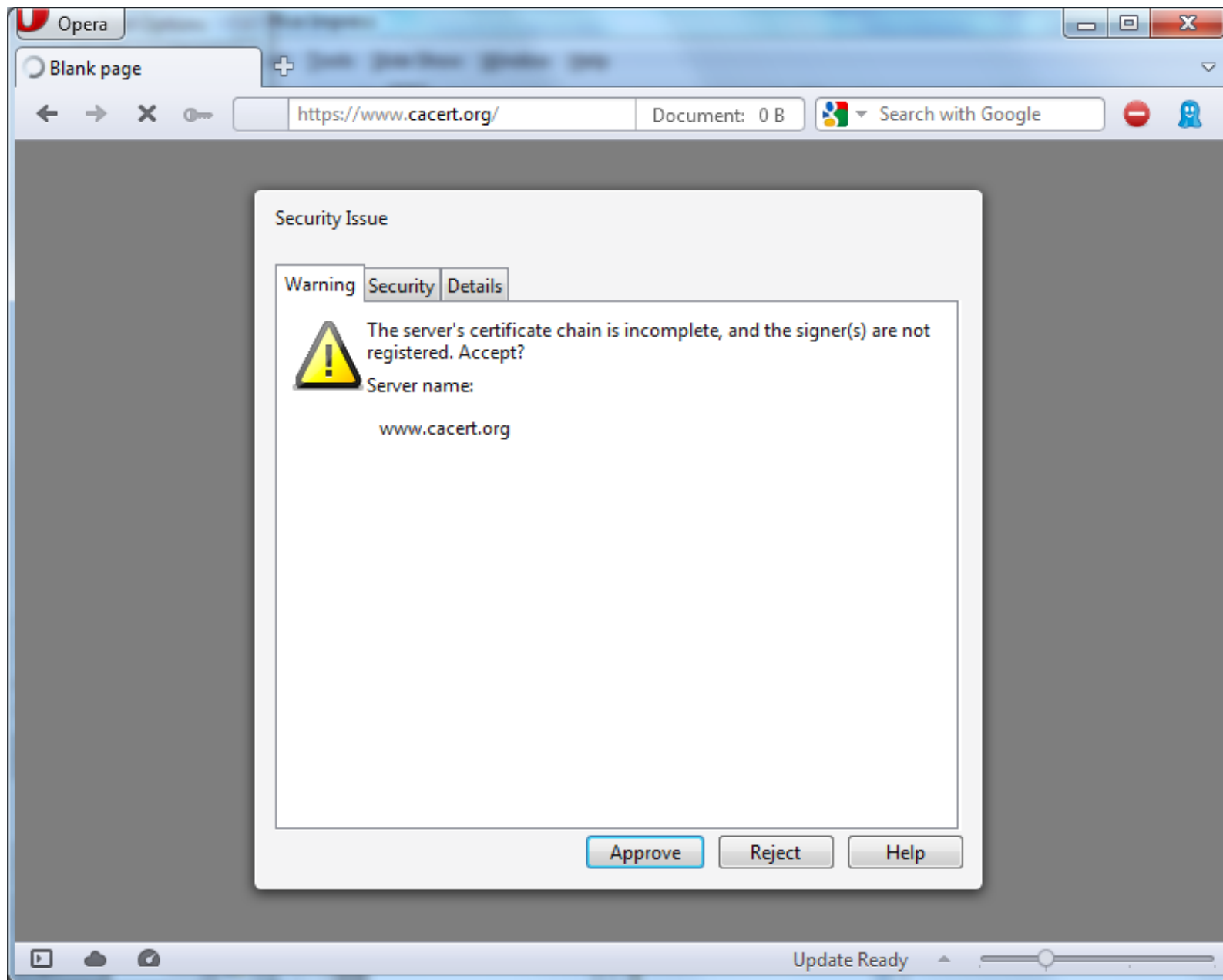
# Сертификат не ОК: Bank of Ireland



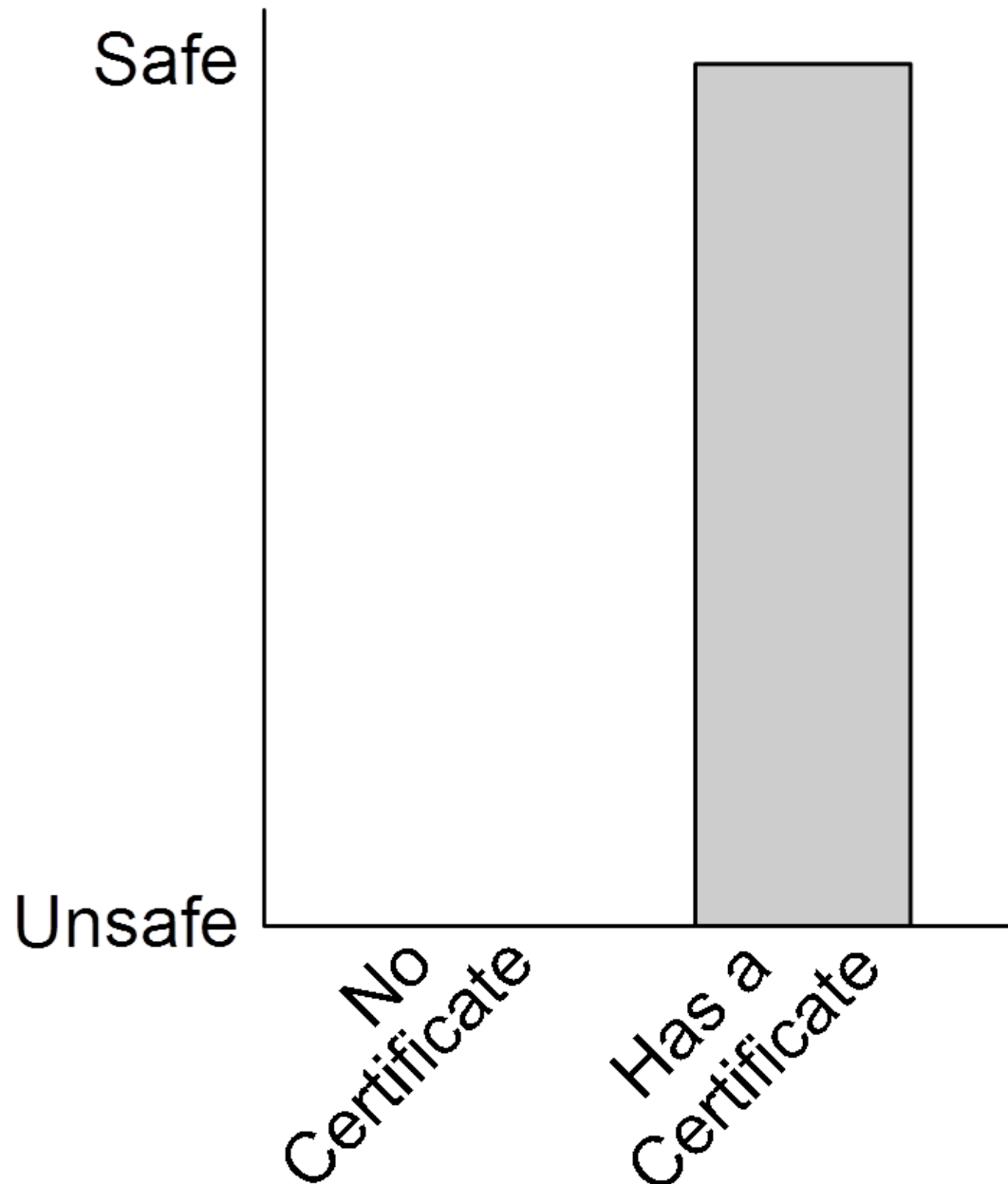
# Сертификат не ОК: VISA



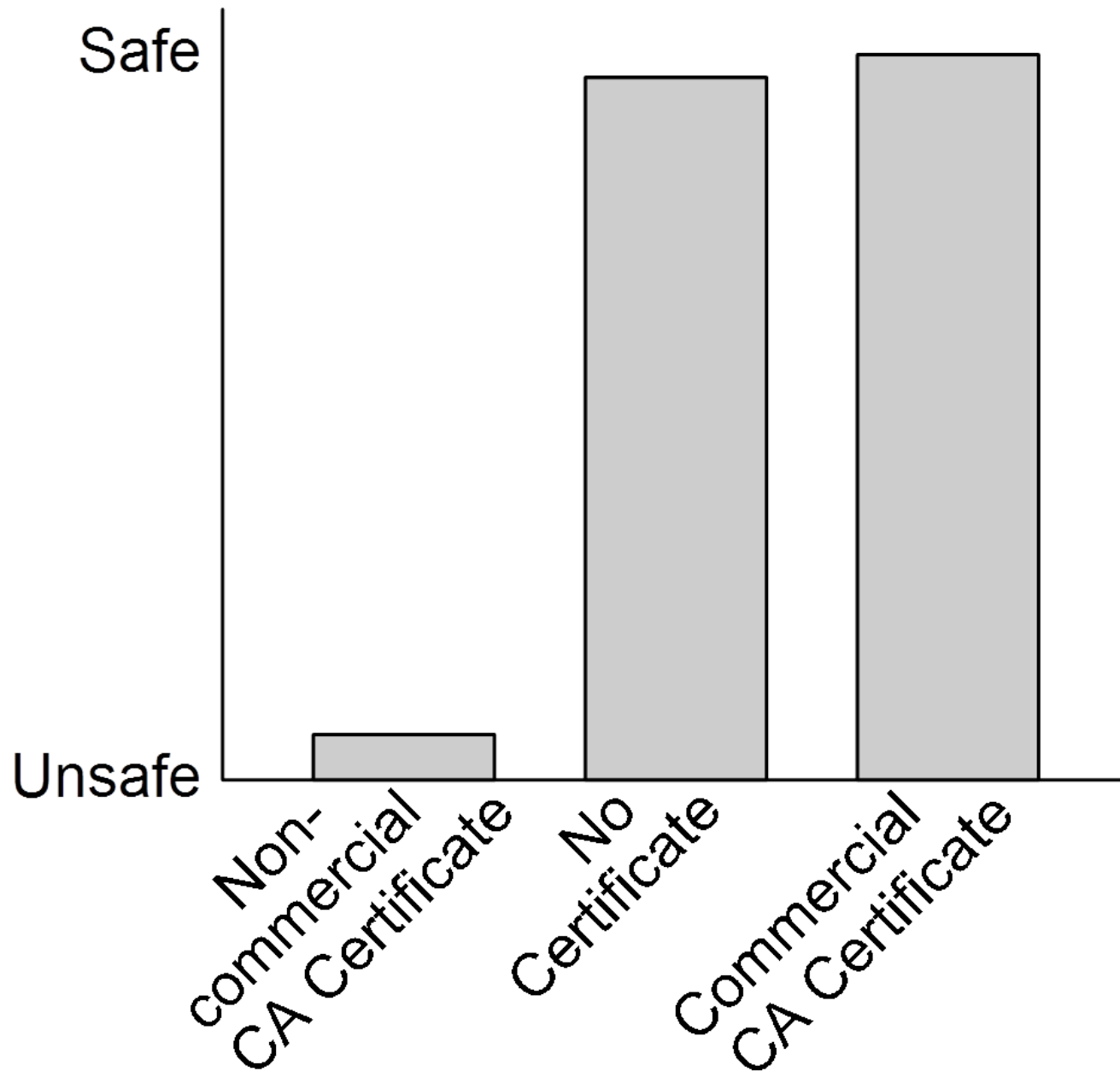
# Некоммерческий СА



# Безопасность в Web: что предполагалось



# Безопасность в Web: что получилось



# Система СА недостаточно надёжна

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



# Система СА недостаточно надёжна

- [sslcertificates@live.com](mailto:sslcertificates@live.com)

# Система СА недостаточно надёжна

- [sslcertificates@live.com](mailto:sslcertificates@live.com)
- Взломы СА: Comodo, Diginotar, Verisign

# Система СА недостаточно надёжна

- [sslcertificates@live.com](mailto:sslcertificates@live.com)
- Взломы СА: 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



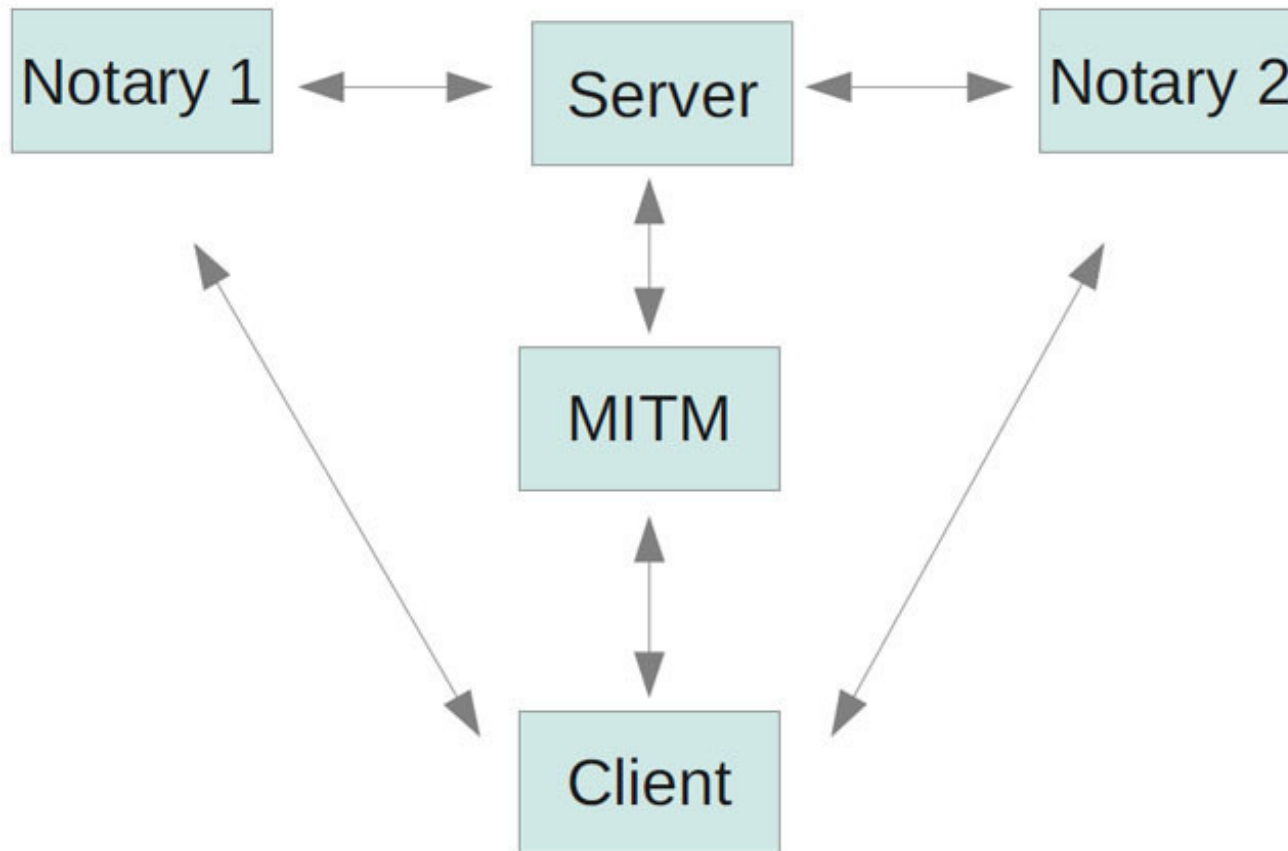
# Чем отвечает индустрия

- HTTP Public Key Pinning (HPKP) и TACK



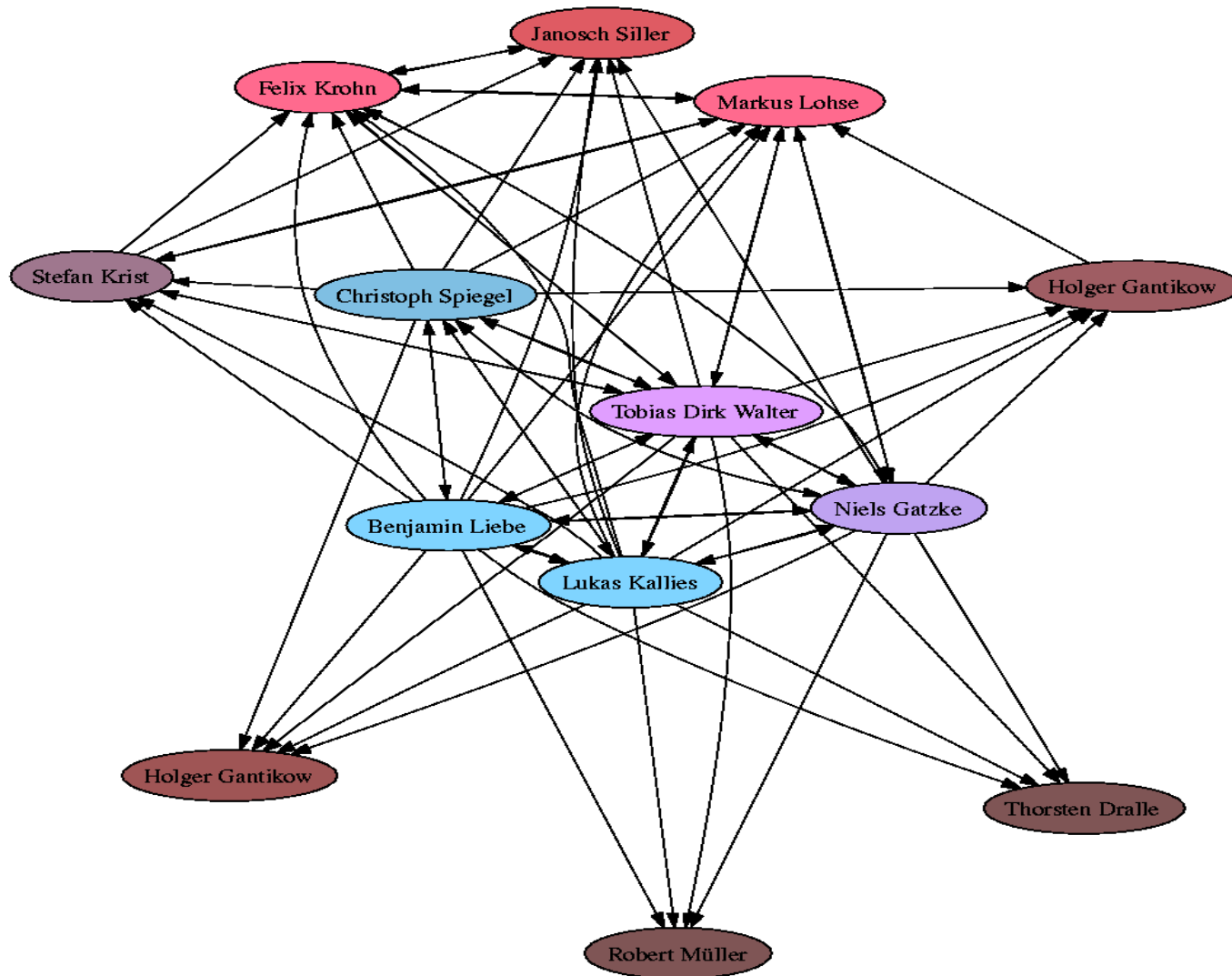
# Чем отвечает индустрия

- Convergence и Mutually Endorsing CA Infr.



# Чем отвечает индустрия

- The Monkeysphere Project и Web of Trust



# PKI them harder



Молотку всё кажется гвоздём





# РКІ – 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:

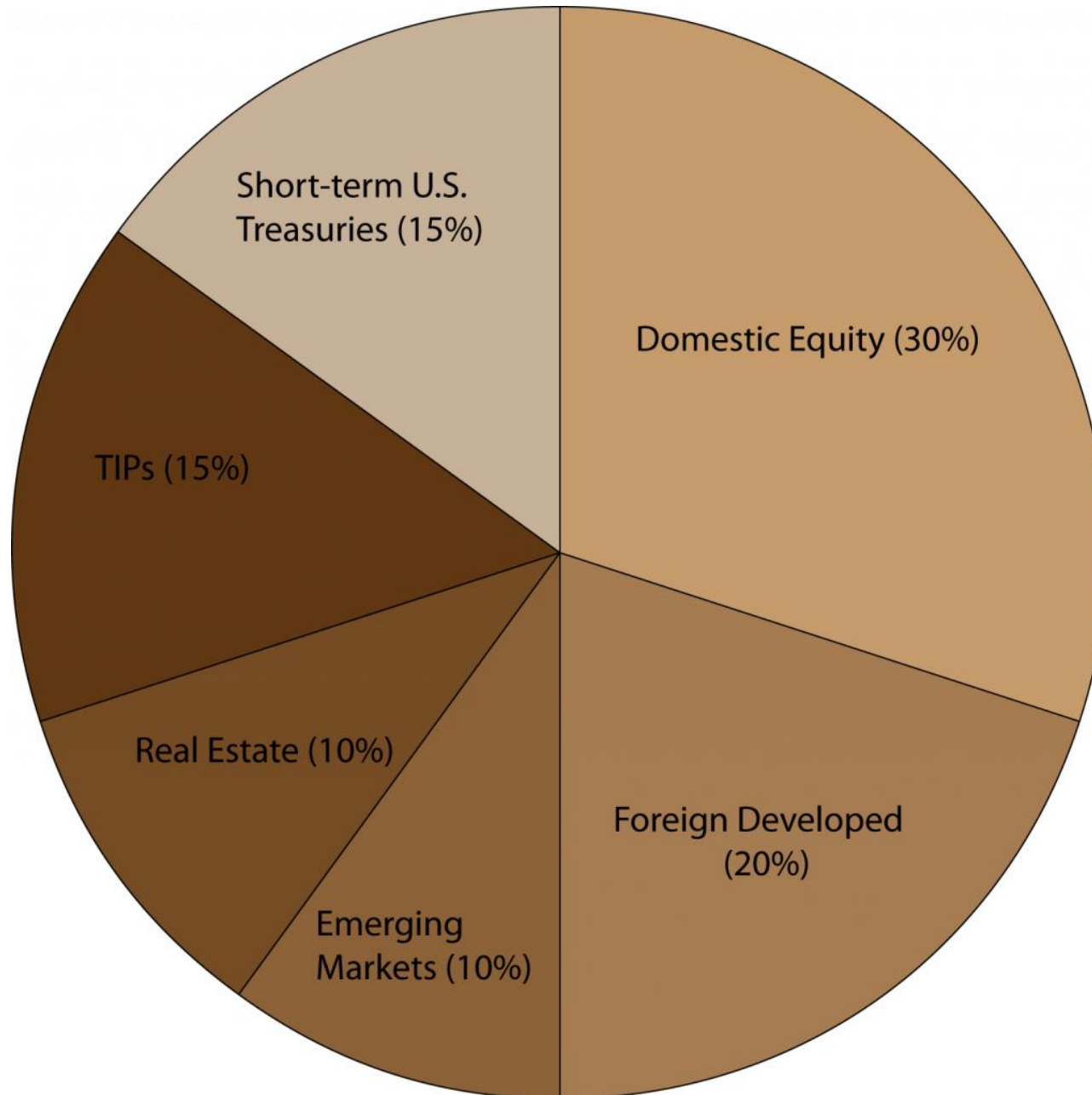
“Управление рисками означает выполнение сознательных действий, направленных на повышение вероятности хорошего исхода дела и уменьшение вероятности плохого исхода дела”

– 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

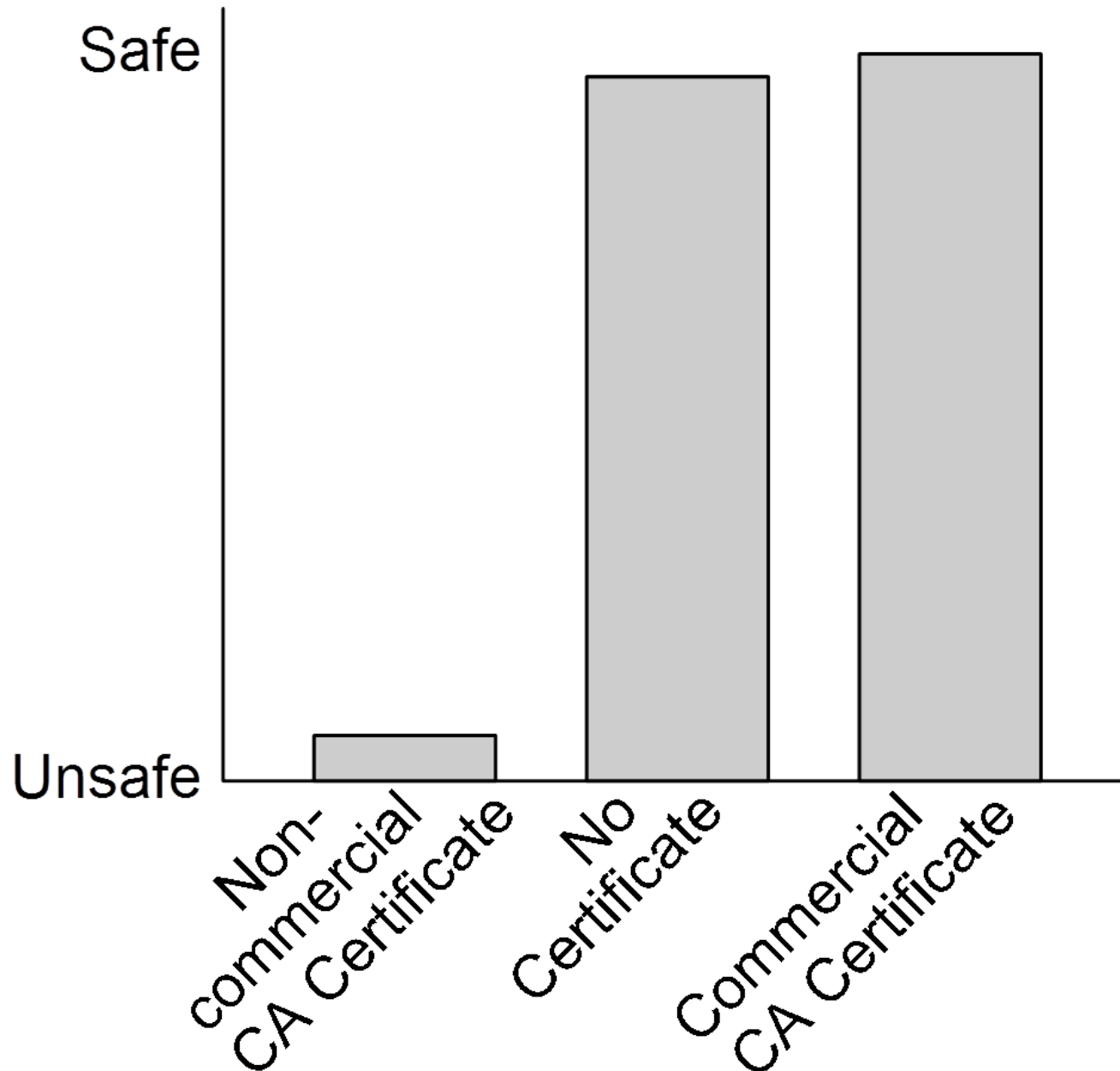
- Лianas против граффити



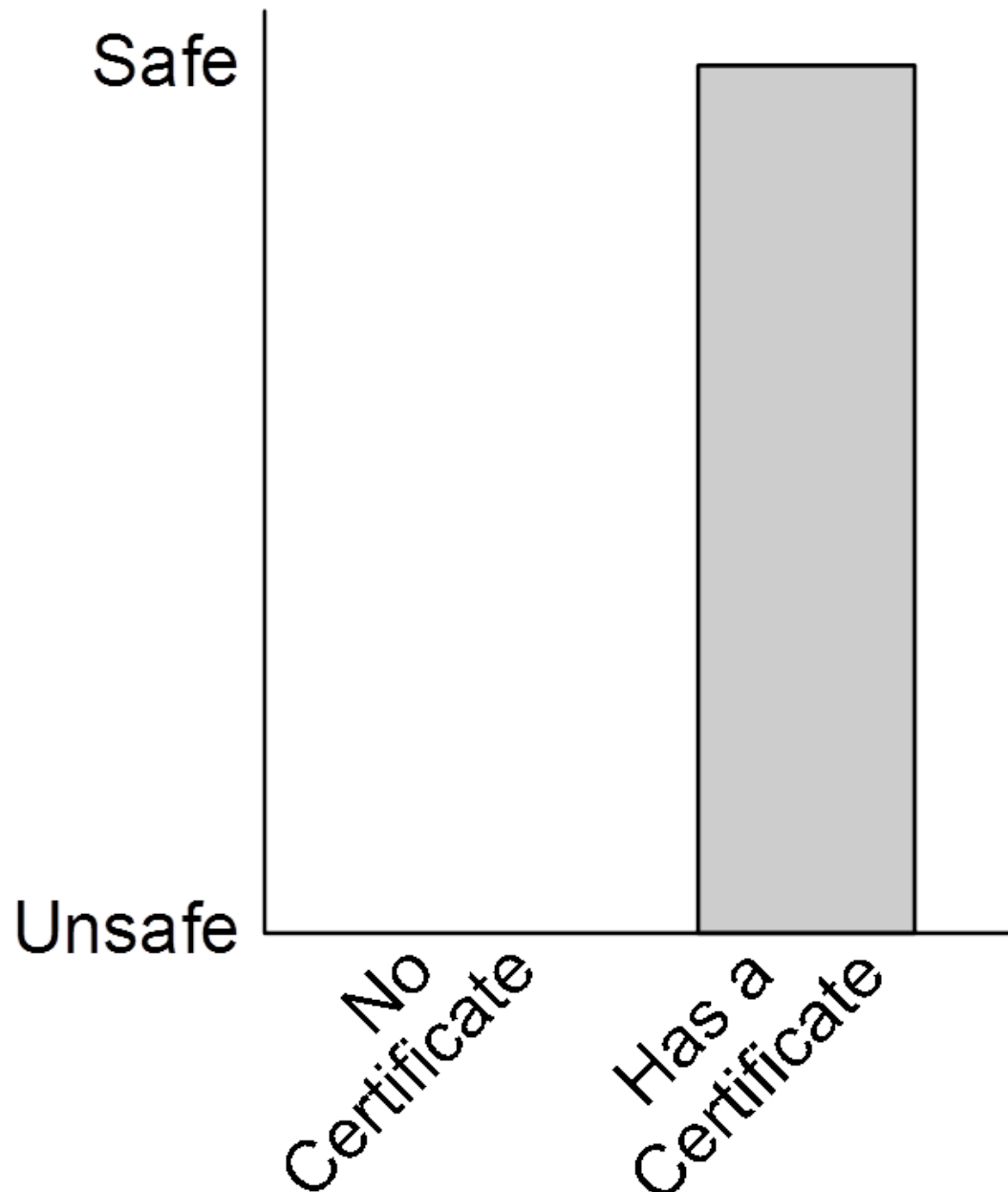
# Безопасность через управление рисками

- 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 TASK, 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 СА

- 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



A screenshot of a web dialog box. At the top, there are two input fields: the first is labeled "Name" and the second is labeled "Password". To the right of these fields is a circular button with the text "OK". Below the input fields, there is a paragraph of text: "Your password will be sent **securely encrypted** to the site **www.paypal.com**, which you've used 25 times in the past". At the bottom of the dialog, there are two rectangular buttons: "Send password" and "Don't send".

# Безопасность через управление рисками

- История взаимодействия с сайтом

Name

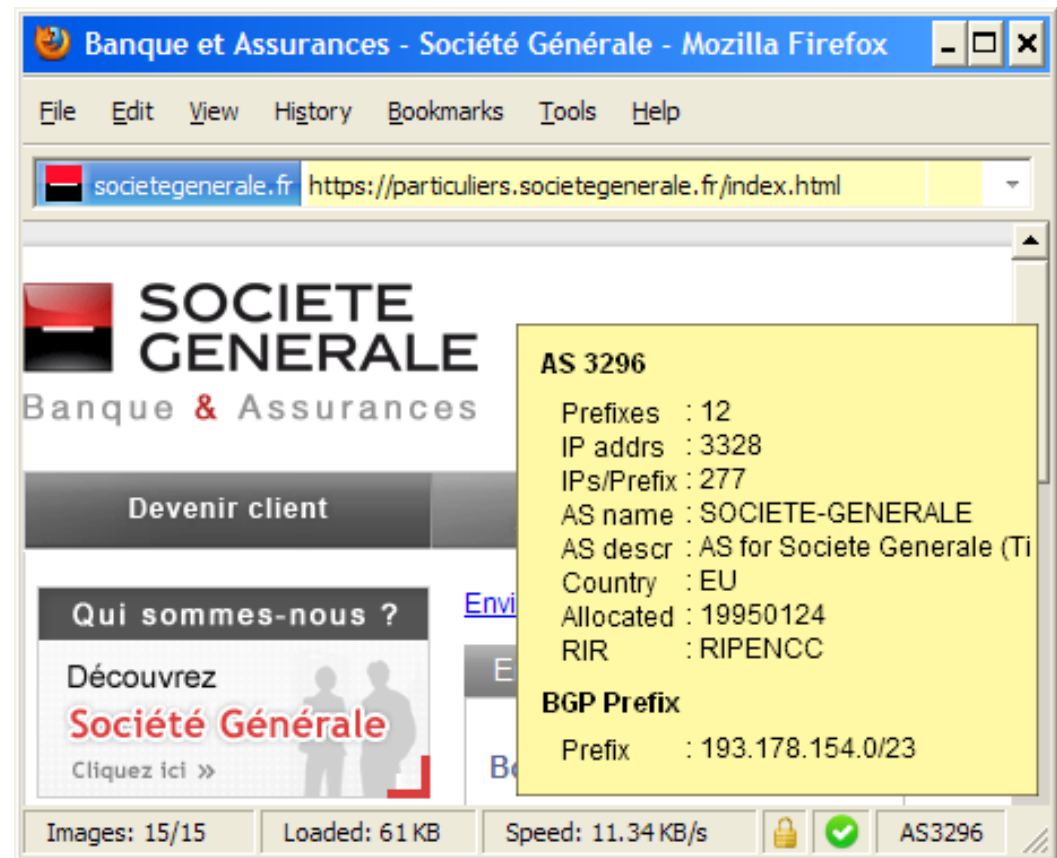
Password



Your password will be sent **without any protection** to the site **www.p4ypa1.com**, which you've never visited before. You should not send your password to this site unless you're absolutely sure that it's safe

# Безопасность через управление рисками

- ХОСТИНГ
  - Whois
  - AS (autonomous system) info



The screenshot shows a Mozilla Firefox browser window titled "Banque et Assurances - Société Générale - Mozilla Firefox". The address bar displays "societegenerale.fr" and the URL "https://particuliers.societegenerale.fr/index.html". The page content includes the Société Générale logo and the text "Banque & Assurances". A yellow overlay box on the right side of the page displays the following information:

**AS 3296**  
Prefixes : 12  
IP addr : 3328  
IPs/Prefix : 277  
AS name : SOCIETE-GENERALE  
AS descr : AS for Societe Generale (Ti  
Country : EU  
Allocated : 19950124  
RIR : RIPENCC

**BGP Prefix**  
Prefix : 193.178.154.0/23

The browser's status bar at the bottom shows "Images: 15/15", "Loaded: 61 KB", "Speed: 11.34 KB/s", and "AS3296".

# 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](http://yandex.ru)
- Spell-check: [panascanic.com](http://panascanic.com), [bankofireland.ie](http://bankofireland.ie)
- Подстроки: “members”, “adsl-pool”, etc



# Безопасность через управление рисками

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



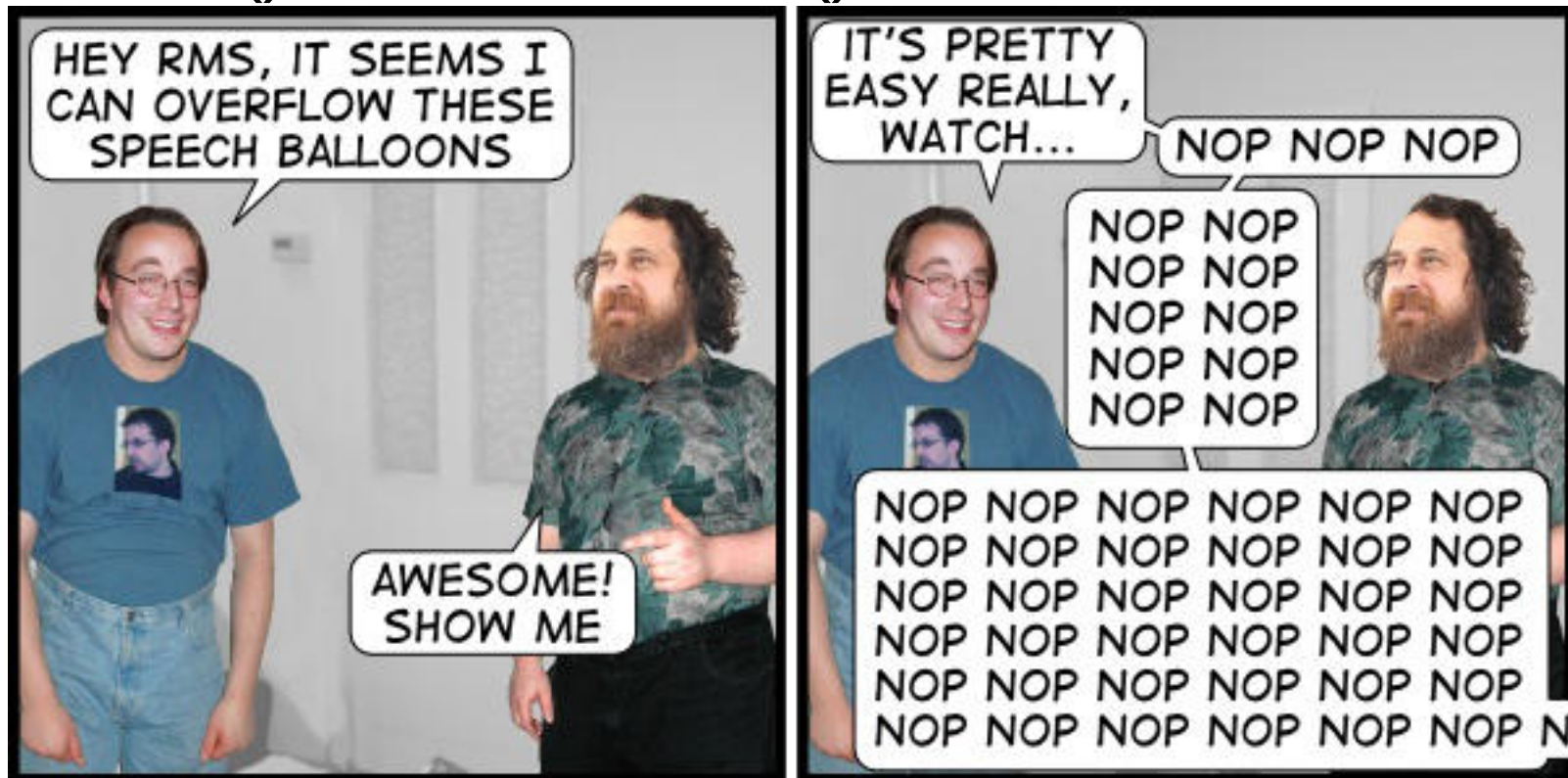
# Безопасность через управление рисками

- 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

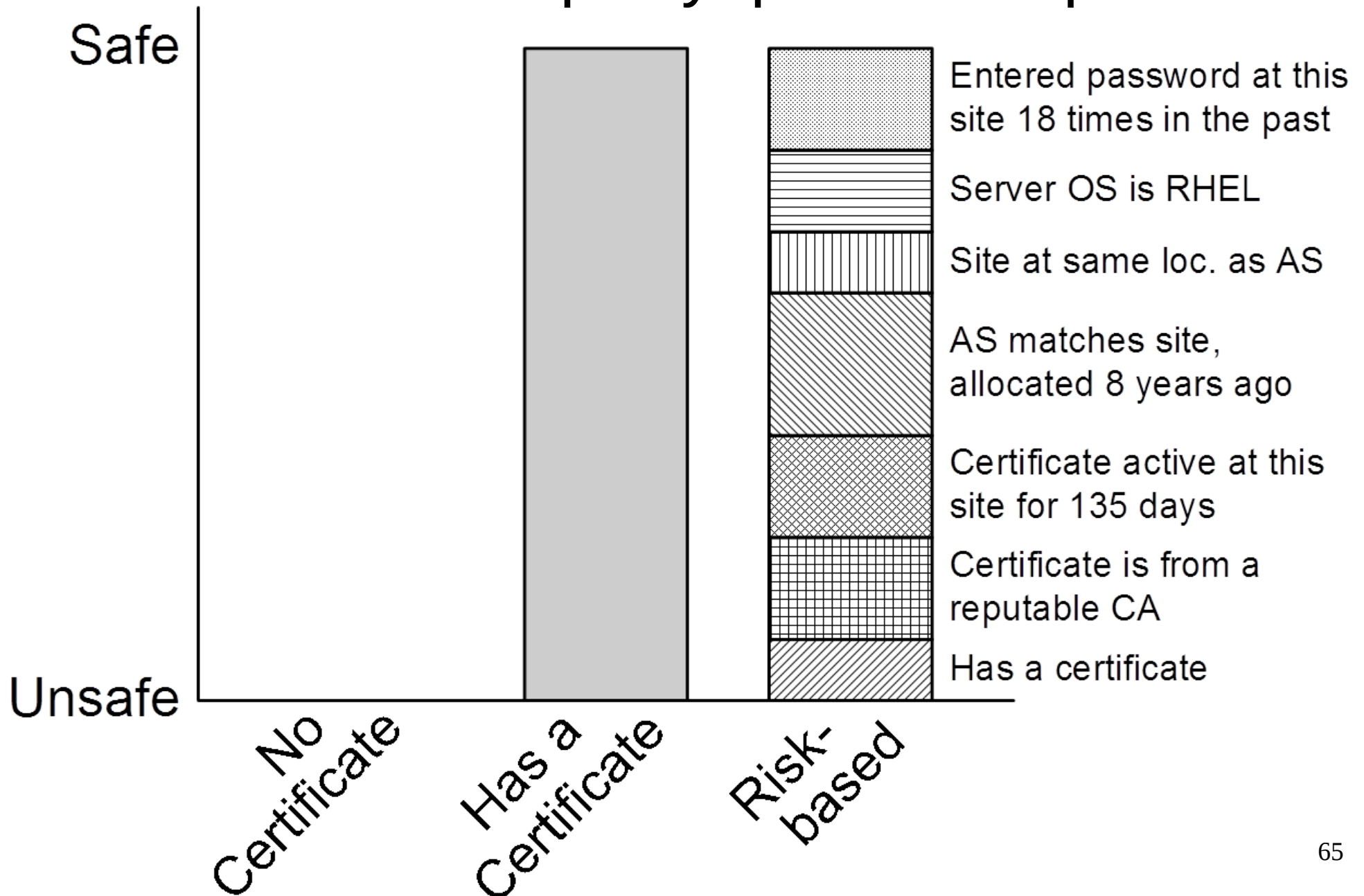


Reverend Thomas Bayes

# 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?