hosting UKRAINE

ХОСТИНГ и РЕГИСТРАЦИЯ ДОМЕНОВ

DNSSEC. Implementation: Why it is so slow.

DNSSEC. Внедрение: Почему так медленно.

Olha Vasylevych, Hosting Ukraine LLC

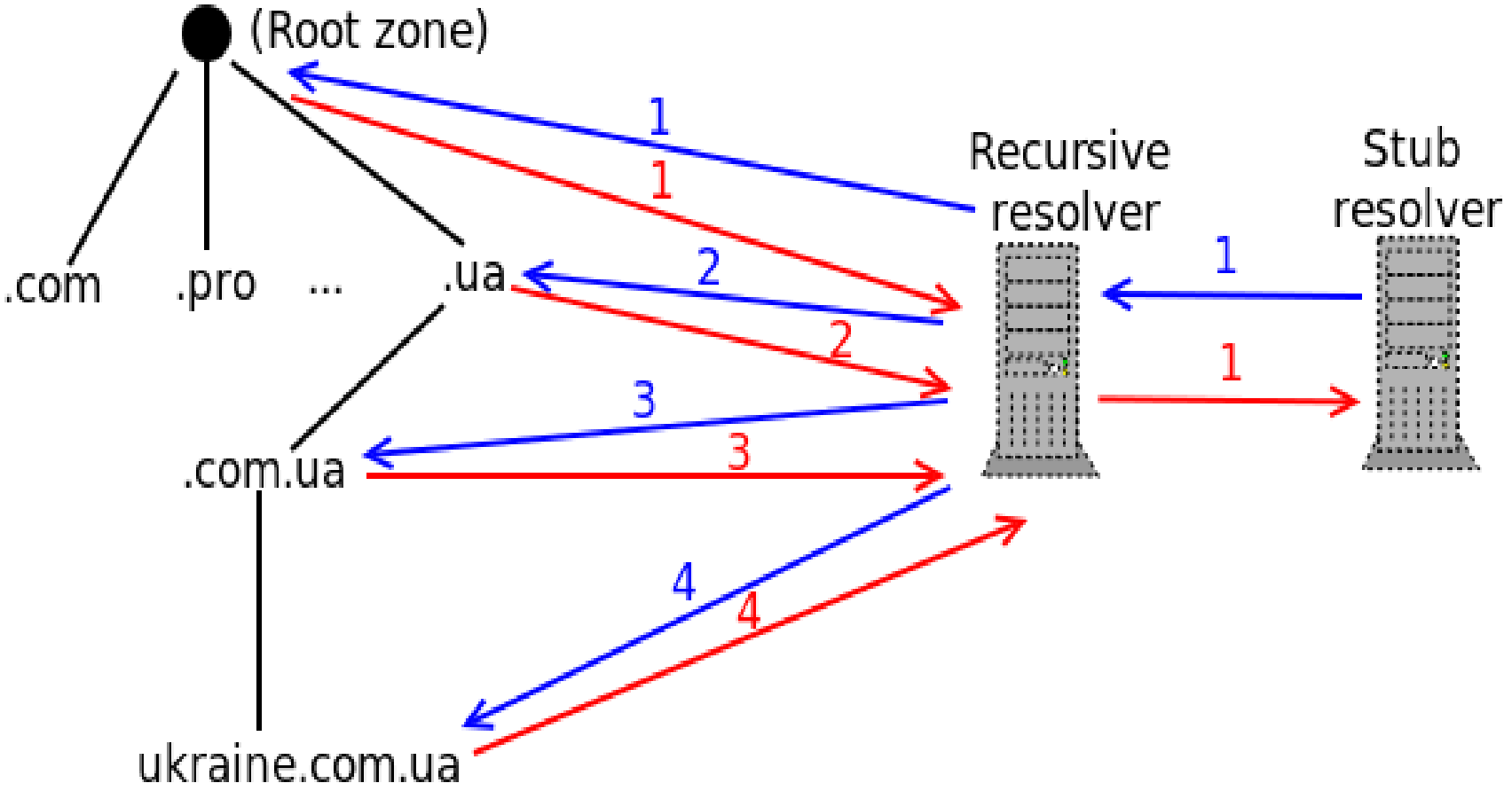
Ольга Василевич, Хостинг Украина

DNS

www.ukraine.com.ua → 185.39.224.12

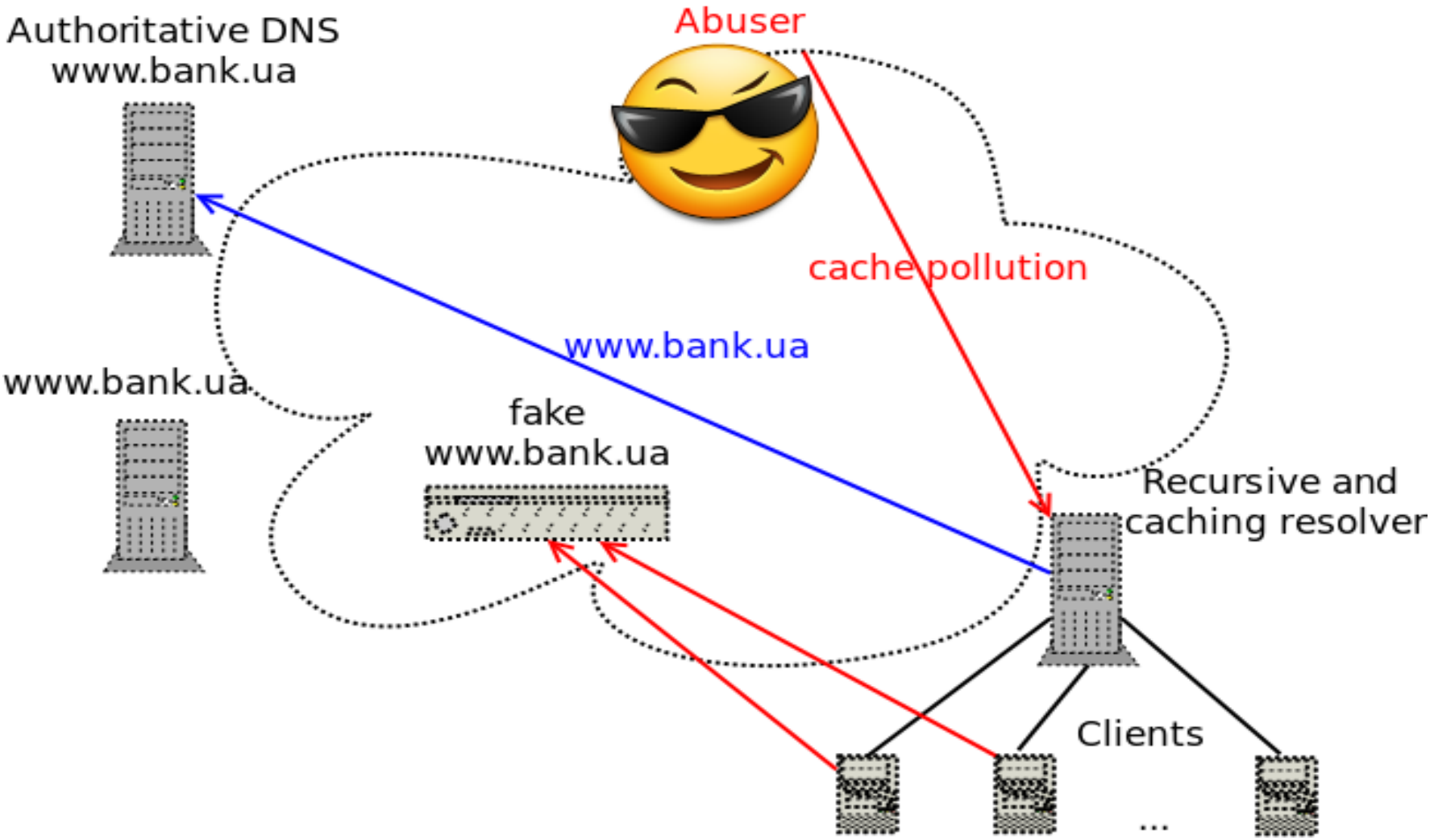
www.ukraine.com.ua → 2a04:8000:0:e00b::2

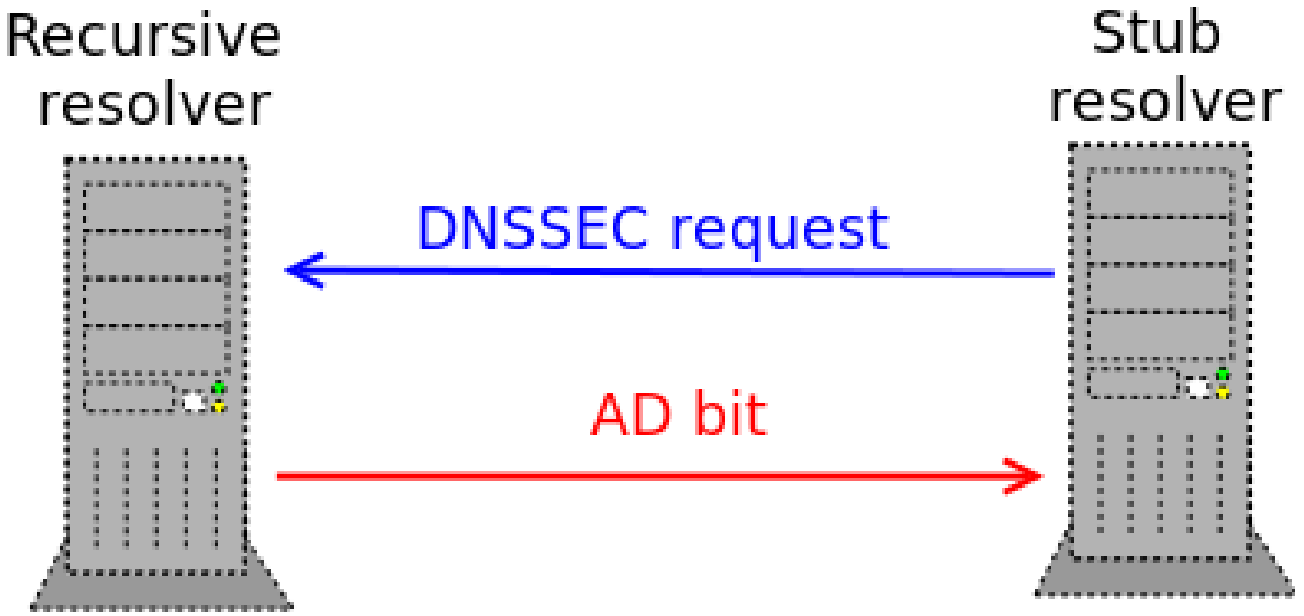
Дерево днс и ресолверы
DNS servers and resolvers



Кеширующий резолвер
Caching resolver

Загрязнение кеша
Cache pollution





;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45667

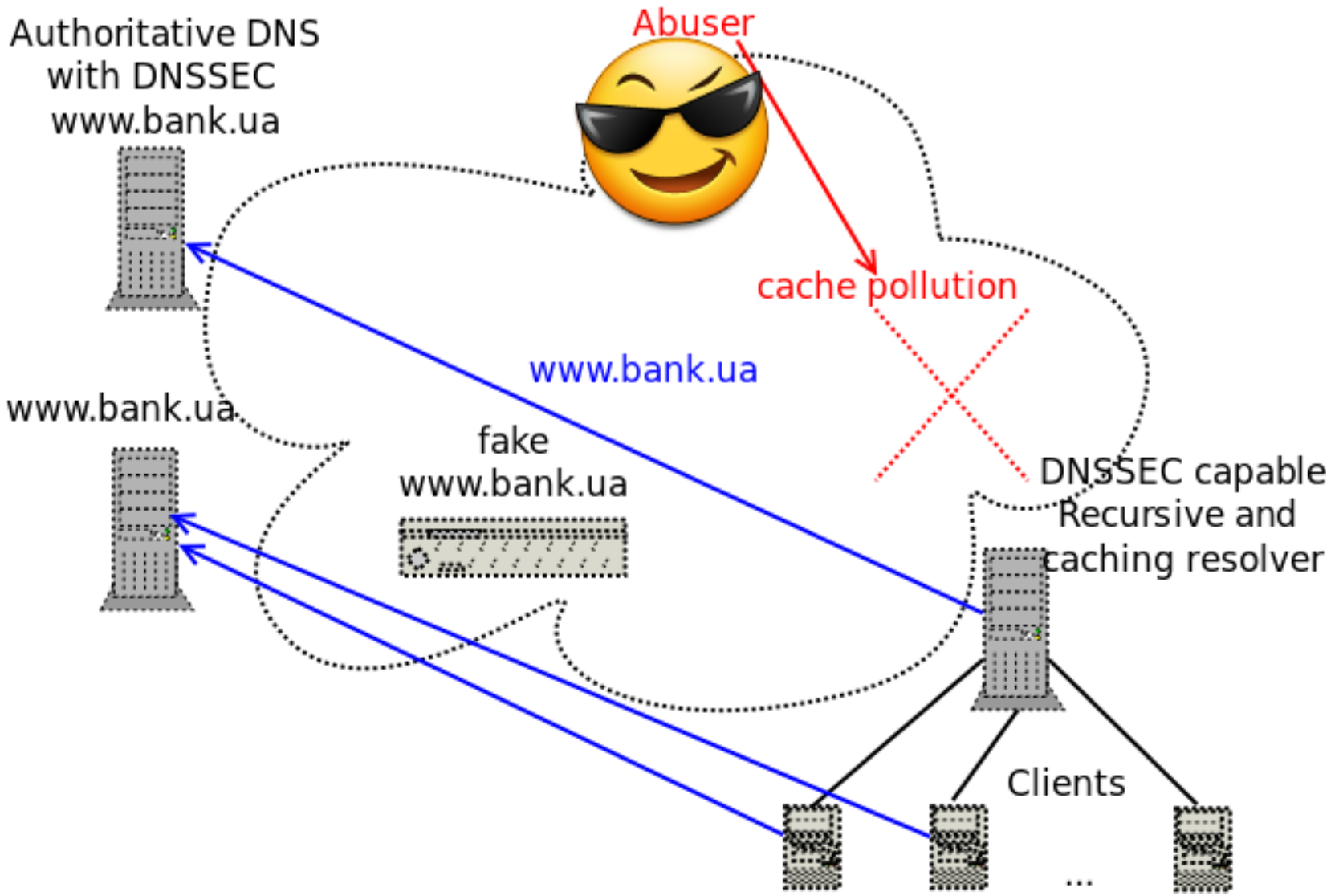
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 13

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags: do; udp: 4096

•

DNSSEC


Authoritative DNS
with DNSSEC
www.bank.ua
Abuser
cache pollution
www.bank.ua
www.bank.ua
fake
www.bank.ua
DNSSEC capable
Recursive and
caching resolver
Clients
...

Общие черты HTTPS и DNSSEC
Common features of HTTPS and DNSSEC

- Оба протокола HTTPS и DNSSEC - это расширение к текствым протоколам HTTP и DNS

  Both protocols HTTPS and DNSSEC are extension for plain-text protocols HTTP and DNS

- Оба расшинения используют ассиметричное шифрование с открытым ключем

  Both extensions use asymetric encryption wit public key

- Оба разабатываются с 90-х годов прошлого века

  Both protocols are in development since 90-ies of the last century

Personal data capturing in HTTP and DNS
Перехват персональных данных в HTTP и DNS

HTTP

- Прослушивание среды передачи данных

  Trafic capturing in the media

- *Man in the middle*
- Сбор всех типов персональных данных для всех сайтов

  Collection of all types of personal data for all sites

DNS

- Выбор цели атаки, создание клона web-сайта и его запуск

  Choose of the victim, web-site clone developement

- Атака с целью загрязнения кеша DNS

  Dns-cache pollution attack

- Man in the middle
- Подмена DNS пакета по перенаправлению на сайт злоумышленника

  DNS spoofing and redirection to the abuser website

- Сбор данных на сайте-клоне

  Data collection with clone web-site

Проблемы внедрения
Implementation problems

HTTPS

На стороне хостинг провайдера, ограничение протокола TLS. 1 IP – 1 ssl host. Решена с помощью расширения протокола SNI

На стороне пользователя:

- Иннертность пользователей решена разработчиками браузеров

DNSSEC

На стороне регистратора доменов:

а) Нет запоса от клиентов

б) Трудоемкий процесс автоматизации решения

На стороне пользователя:

а) Нет решения валидации DNSSEC из коробки

б) ISP и производители оборудования не стремятся включать DNSSEC валидацию на своих устройствах

DNSSEC validators
Приложения для проверки подлинности DNSSEC

https://www.dnssec-validator.cz

http://www.nlnetlabs.nl/projects/dnssec-trigger/

Причины медленного внедрения DNSSEC
Reasons of slow implementation

1) Нет массового запроса от пользователей из-за сложности понимания технологии.

End-user request is absent for DNSSEC.

2) Ресурсозатратность для операторов и Интернет-провайдеров, дополнительное администрирование, дополнительное оборудаование для обеспечения работы DNSSEC.

DNSSEC implementation brings for operators additional administrative costs and additional equipment installation.

3) У DNS-операторов нет стимула, так как нет запроса от пользователей на услугу.

DNS-operators do nto have stimul, as no request.

4) В отличии от HTTPS внедрение DNSSEC происходит сверху вниз, то есть инициаторами внедрения выступают общественные организации и рабочие группы специалистов по Интернет технологиям, а не конечные пользователи сети, которые платят деньги Интернет-провайдерам, регистраторам доменов и провайдерам хостинга.

Initiative of DNSSEC implementation does from “top to bottom”. It belongs to the public organizations and working groups of proffesionals in Internet tecnologies, but not from the end-users, who pays money to ISPs, Registars and hosting providers.

Как повысить интерес к DNSSEC конечного пользователя?
How to rise interest of end-user to DNSSEC?

Разработчикам браузеров внедрить проверку DNSSEC в браузеры в базовой конфигурации, так как конечные пользователи не видят реальной работы DNSSEC.

Browser developers should implement DNSSEC validation “form the box”, otherwithe end-users do not see real work of DNSSEC.

Но особенность данного предложения заключается в том, что если валидатор DNSSEC выводить пользователям в браузер, то нужно так же устанавливать на устройство рекурсивный DNS резолвер с поддержкой DNSSEC, как и предложено в RFC3655(Redefinition of DNS AD bit).

But in this case recursive DNS validator should be installed on the client device also, as was recommended in the RFC3555(Redefinition of DNS AD bit).

Спасибо!
Thank you!

DNSSEC. Implementation: Why it is so slow.

DNSSEC. Внедрение: Почему так медленно.

Olha Vasylevych, Hosting Ukraine LLC

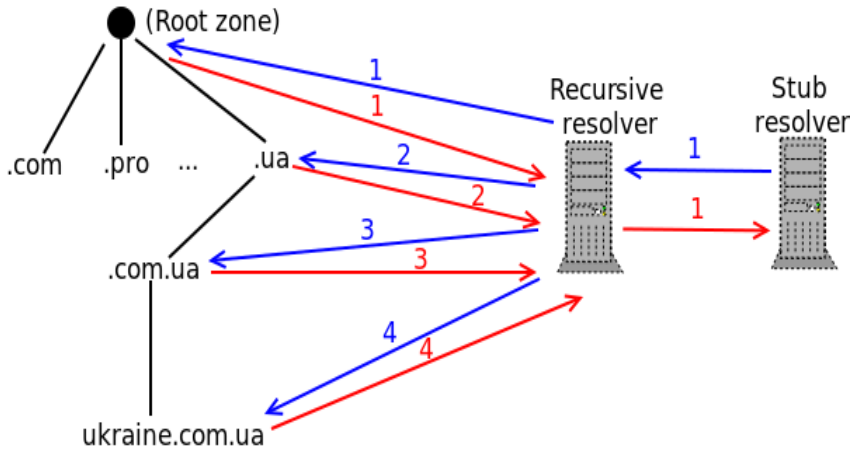
Ольга Василевич, Хостинг Украина

DNS

www.ukraine.com.ua → 185.39.224.12

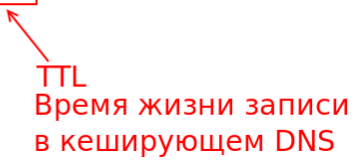
www.ukraine.com.ua → 2a04:8000:0:e00b::2

Дерево днс и ресолверы
DNS servers and resolvers

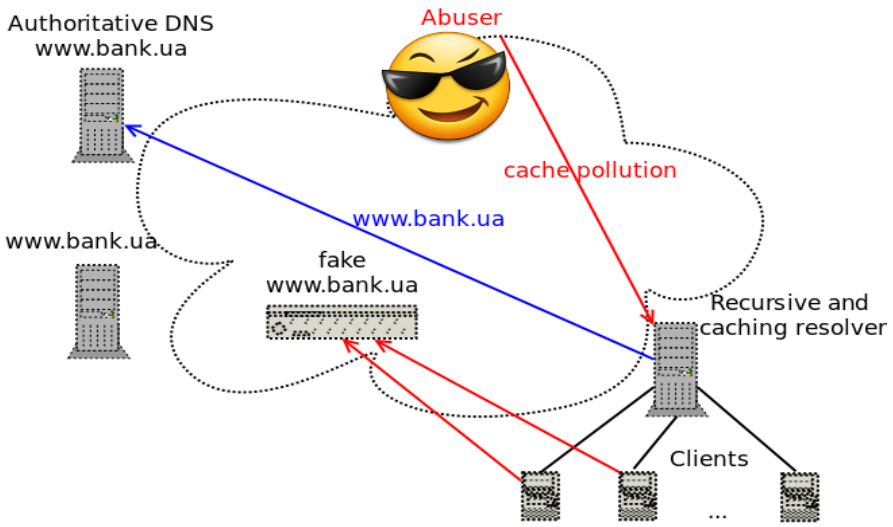


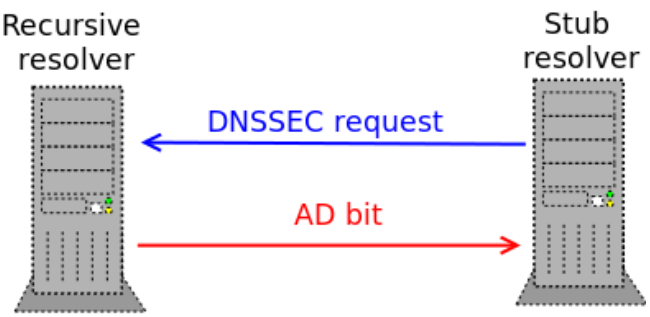
Кеширующий резолвер
Caching resolver

www.ukraine.com.ua. 900 IN A 185.39.224.12



Загрязнение кеша
Cache pollution



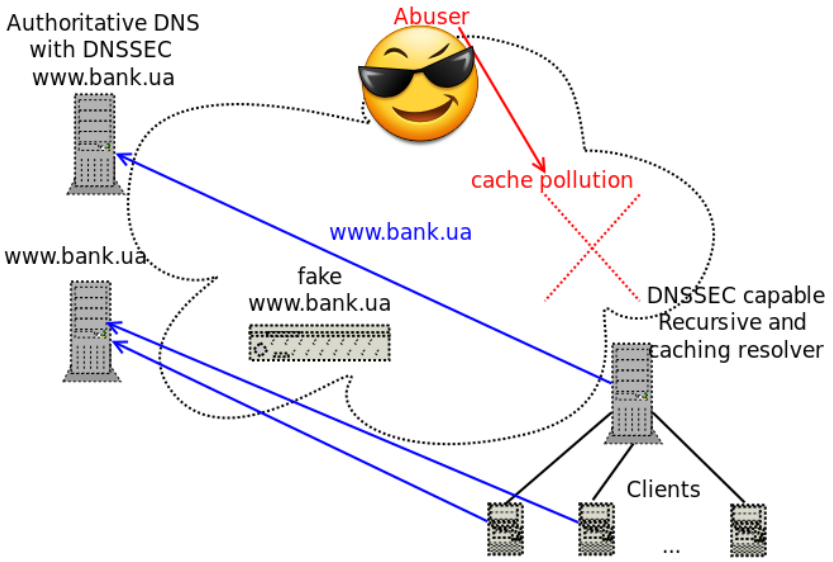


;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45667
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096

•

DNSSEC


Authoritative DNS
with DNSSEC
www.bank.ua
Abuser
cache pollution
www.bank.ua
www.bank.ua
fake
www.bank.ua
DNSSEC capable
Recursive and
caching resolver
Clients
...

Общие черты HTTPS и DNSSEC
Common features of HTTPS and DNSSEC

- Оба протокола HTTPS и DNSSEC - это расширение к текствым протоколам HTTP и DNS

  Both protocols HTTPS and DNSSEC are extension for plain-text protocols HTTP and DNS

- Оба расшинения используют ассиметричное шифрование с открытым ключем

  Both extensions use asymetric encryption wit public key

- Оба разабатываются с 90-х годов прошлого века

  Both protocols are in development since 90-ies of the last century

Personal data capturing in HTTP and DNS
Перехват персональных данных в HTTP и DNS

HTTP

- Прослушивание среды передачи данных

  Trafic capturing in the media

- *Man in the middle*
- Сбор всех типов персональных данных для всех сайтов

  Collection of all types of personal data for all sites

DNS

- Выбор цели атаки, создание клона web-сайта и его запуск

  Choose of the victim, web-site clone developement

- Атака с целью загрязнения кеша DNS

  Dns-cache pollution attack

- Man in the middle
- Подмена DNS пакета по перенаправлению на сайт злоумышленника

  DNS spoofing and redirection to the abuser website

- Сбор данных на сайте-клоне

  Data collection with clone web-site

Проблемы внедрения
Implementation problems

HTTPS

На стороне хостинг провайдера, ограничение протокола TLS. 1 IP – 1 ssl host. Решена с помощью расширения протокола SNI

На стороне пользователя:

- Иннертность пользователей решена разработчиками браузеров

DNSSEC

На стороне регистратора доменов:

а) Нет запоса от клиентов

б) Трудоемкий процесс автоматизации решения

На стороне пользователя:

а) Нет решения валидации DNSSEC из коробки

б) ISP и производители оборудования не стремятся включать DNSSEC валидацию на своих устройствах

DNSSEC validators
Приложения для проверки подлинности DNSSEC

https://www.dnssec-validator.cz

http://www.nlnetlabs.nl/projects/dnssec-trigger/

Причины медленного внедрения DNSSEC
Reasons of slow implementation

1) Нет массового запроса от пользователей из-за сложности понимания технологии.

End-user request is absent for DNSSEC.

2) Ресурсозатратность для операторов и Интернет-провайдеров, дополнительное администрирование, дополнительное оборудаование для обеспечения работы DNSSEC.

DNSSEC implementation brings for operators additional administrative costs and additional equipment installation.

3) У DNS-операторов нет стимула, так как нет запроса от пользователей на услугу.

DNS-operators do nto have stimul, as no request.

4) В отличии от HTTPS внедрение DNSSEC происходит сверху вниз, то есть инициаторами внедрения выступают общественные организации и рабочие группы специалистов по Интернет технологиям, а не конечные пользователи сети, которые платят деньги Интернет-провайдерам, регистраторам доменов и провайдерам хостинга.

Initiative of DNSSEC implementation does from “top to bottom”. It belongs to the public organizations and working groups of proffesionals in Internet tecnologies, but not from the end-users, who pays money to ISPs, Registars and hosting providers.

Как повысить интерес к DNSSEC конечного пользователя?
How to rise interest of end-user to DNSSEC?

Разработчикам браузеров внедрить проверку DNSSEC в браузеры в базовой конфигурации, так как конечные пользователи не видят реальной работы DNSSEC.

Browser developers should implement DNSSEC validation “form the box”, otherwithe end-users do not see real work of DNSSEC.

Но особенность данного предложения заключается в том, что если валидатор DNSSEC выводить пользователям в браузер, то нужно так же устанавливать на устройство рекурсивный DNS резолвер с поддержкой DNSSEC, как и предложено в RFC3655(Redefinition of DNS AD bit).

But in this case recursive DNS validator should be installed on the client device also, as was recommended in the RFC3555(Redefinition of DNS AD bit).

Спасибо!
Thank you!