DNS Security

Agenda

1. DNS protocol security
2. Extensions to the protocol
3. DNS system security
4. Domain owner privacy

Domain Name System

- Naming system for computers (example.com → IP address)
- Hierarchical (subdomain.example.com)
- Distributed database
- Used since 1985

Use cases

- Web browsing
- Sending emails
- … anything that uses internet

DNS Protocol

Query

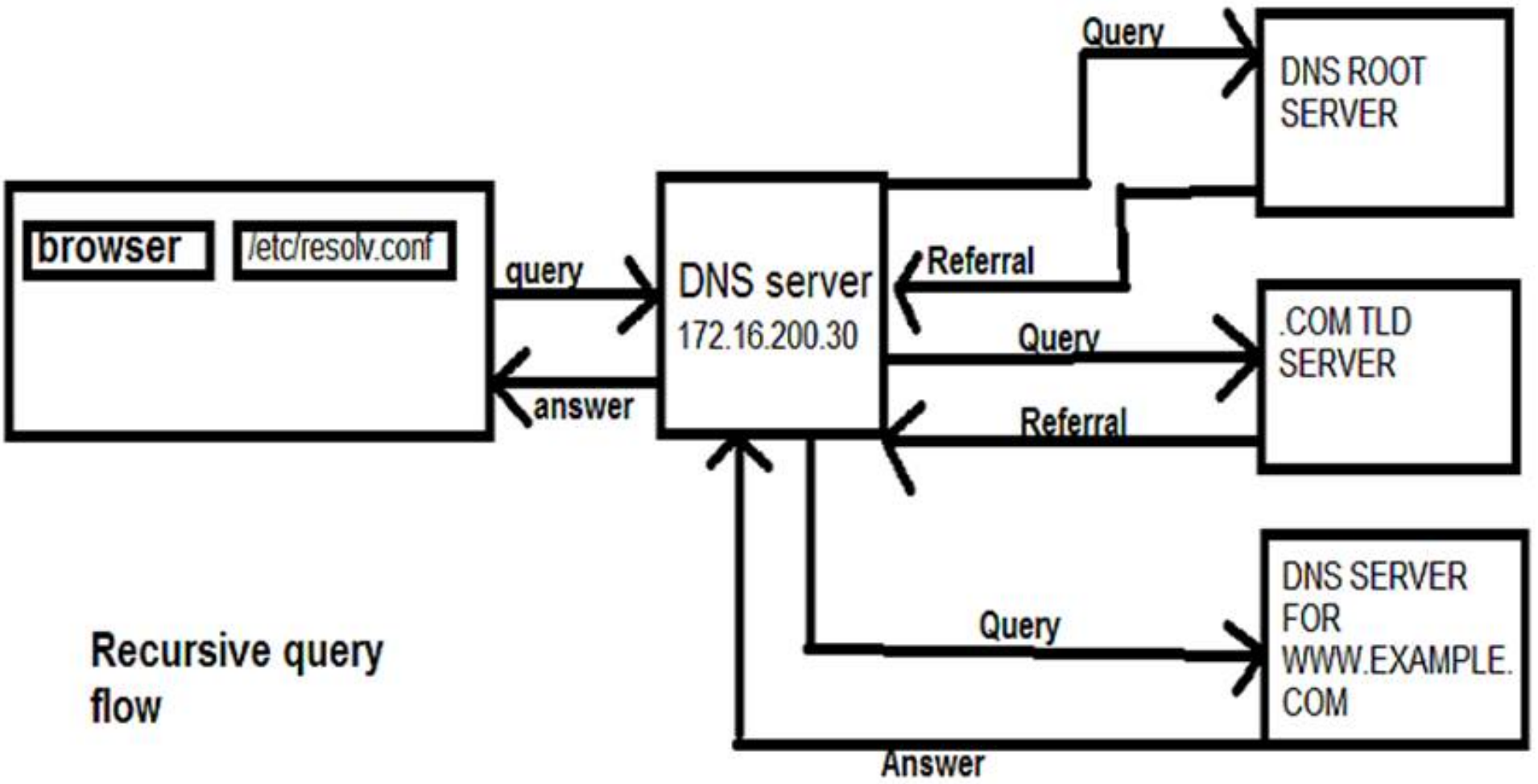
```
int getaddrinfo(const char *node, const char *service,
                const struct addrinfo *hints,
                struct addrinfo **res);
```

- Check local hosts file
- Check local cache
- If not found, query DNS server

Server Structure

- Hierarchical server structure
  - root – point to TLD servers
  - Top level domain (TLD) – point to domain servers
  - Domain servers
- Servers use caching

Query Path


Query
DNS ROOT SERVER
browser
/etc/resolv.conf
query
DNS server
172.16.200.30
Referral
Query
.COM TLD SERVER
answer
Referral
DNS SERVER FOR WWW.EXAMPLE.COM
Query
Answer
Recursive query flow

Which DNS server

- OS - knows IP of two DNS servers (configurable)
- Typically, computers query gateway address (192.168.1.1)
- Routers query ISP DNS servers (orange etc.)

What could possibly go wrong

What could possibly go wrong

- Modified hosts file
- “Rogue” DNS servers
  - untrusted wifi
  - ISP banning certain websites

ISP blocking

Uwaga!

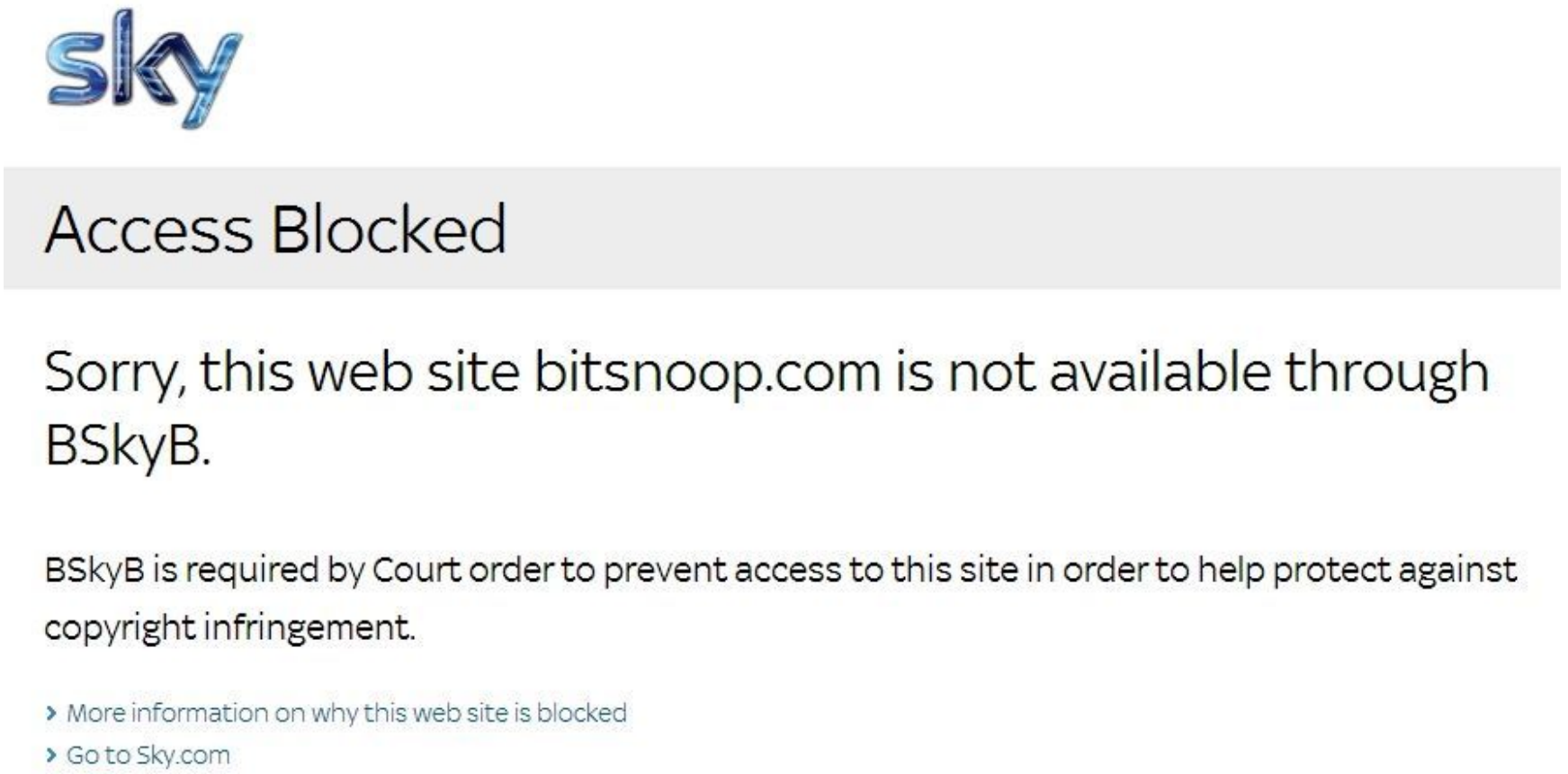
Strona internetowa, z którą podjęto próbę połączenia jest wykorzystywana do nielegalnego oferowania gier hazardowych.

Dostęp do strony został zablokowany na podstawie art. 15f ustawy z dnia 19 listopada 2009 r. o grach hazardowych, zgodnie z którym Minister Rozwoju i Finansów prowadzi Rejestr Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą podlegających blokowaniu w związku z wpisaniem do Rejestru domeny wykorzystywanej przez stronę internetową. Pełna lista nazw domen wpisanych do Rejestru dostępna jest na stronie www.hazard.mf.gov.pl

Uczestnictwo w grach hazardowych urządzanych przez podmioty nieposiadające zezwolenia Ministra Rozwoju i Finansów na prowadzenie działalności w tym zakresie zagrożone jest karą administracyjną i karnoskarbową. Zgodnie bowiem z art. 89 ust. 1 pkt 6 ustawy o grach hazardowych karze pieniężnej podlega uczestnik gry hazardowej urządzanej bez koncesji, bez zezwolenia lub bez zgłoszenia, która zgodnie z art. 89 ust. 4 pkt 5 wynosi 100% uzyskanej wygranej niepomniejszonej o kwoty wpłaconych stawek. Ponadto art. 107 § 2 kodeksu karnego skarbowego przewiduje karę grzywny do wysokości 120 stawek dziennych za uczestniczenie w zagranicznej grze hazardowej, a w art. 109 przewidziano karę grzywny w takiej samej wysokości za uczestniczenie w grze hazardowej urządzanej lub prowadzonej wbrew przepisom ustawy lub warunkom koncesji lub zezwolenia.

Legalne jest uczestniczenie w grach urządzanych przez podmiot posiadający wymagane prawem zezwolenie lub urządzających gry w sieci Internet w ramach monopolu państwa. Lista podmiotów posiadających takie zezwolenie lub uprawnionych do ich urządzania w ramach monopolu państwa dostępna jest na stronie http://www.finanse.mf.gov.pl/inne-podatki/podatek-od-gier/gry-hazardowe-przez-internet.

ISP blocking



Mitigations

- Modify hosts file with caution
- Use trusted DNS servers

Good news

- Block ads
- Block Facebook (and others)

  https://github.com/jmdugan/blocklists/blob/master/corporations/facebook/all

What could possibly go wrong

- ~~Modified hosts file~~
- ~~“Rogue” DNS servers~~
  - ~~untrusted wifi~~
  - ~~ISP banning certain websites~~

Does it really help?

DNS query

- UDP – easy to spoof!
- Destination port 53
- Known format
- Not encrypted

What could possibly go wrong

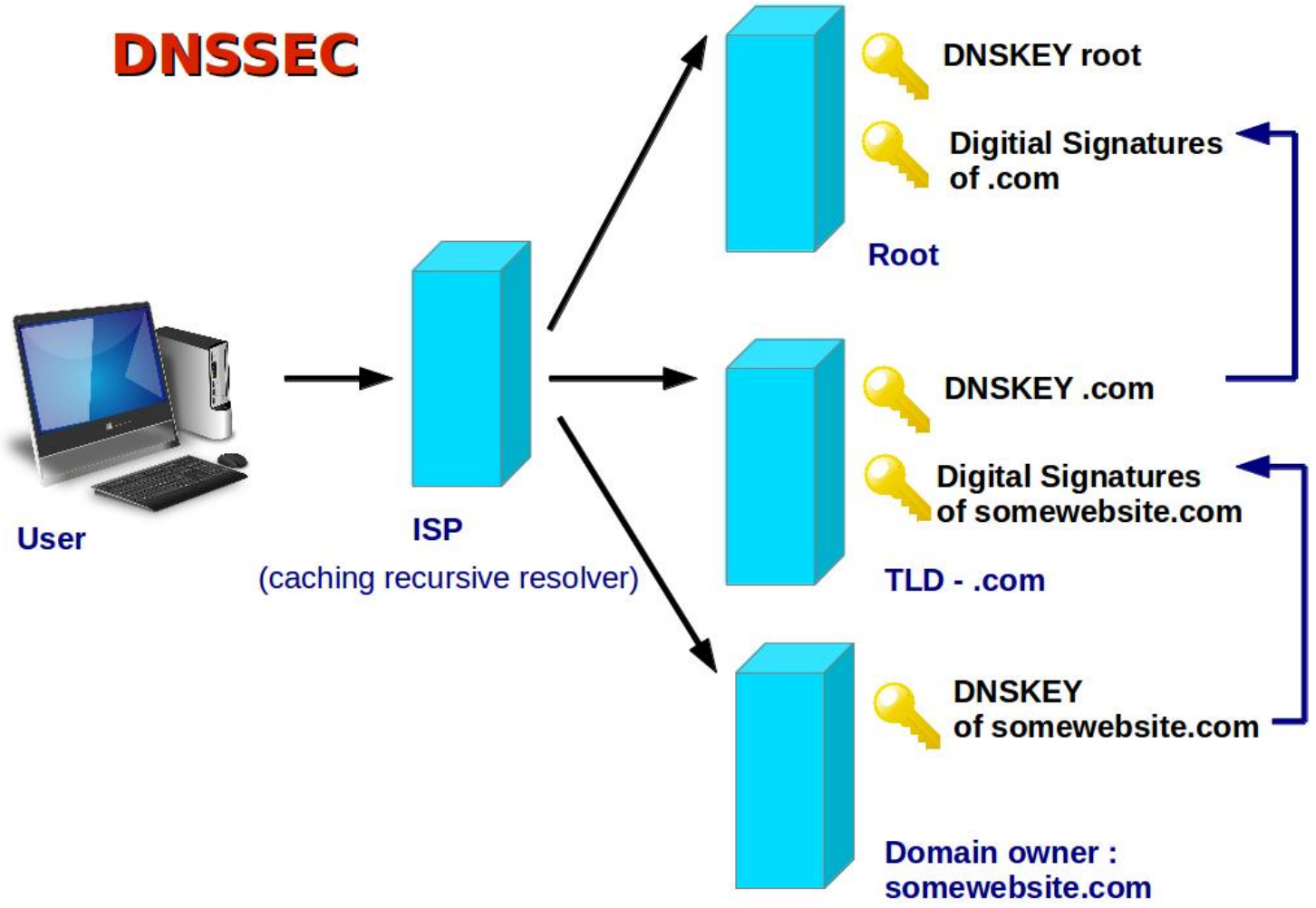
- ~~Modified hosts file~~
- ~~“Rogue” DNS servers~~
  - ~~untrusted wifi~~
  - ~~ISP banning certain websites~~
- router operator/ISP/NSA hijacks DNS packet. Then, it sends back its own response.

DNS extensions

DNSSec

- Signs DNS records
- Public key cryptography
- Uses DNS hierarchy
- Authentication, no encryption
- Created in 1997

DNSSec


DNSSEC
DNSKEY root
Digitial Signatures
of .com
Root
User
ISP
(caching recursive resolver)
DNSKEY .com
Digital Signatures
of somewebsite.com
TLD - .com
DNSKEY
of somewebsite.com
Domain owner :
somewebsite.com

DNSSec adoption

- Most TLDs support it

DNSSec adoption

- Most TLDs support it
- 12% of DNS queries are validated
- *only ~1% of .com, .net and .org domains deploy DNSSEC*
- *Even among the most popular domains, deployment is no more that 1.85% of domains.*

Source (data from August 2016): https://securepki.org/sec17.html

DNSSec adoption

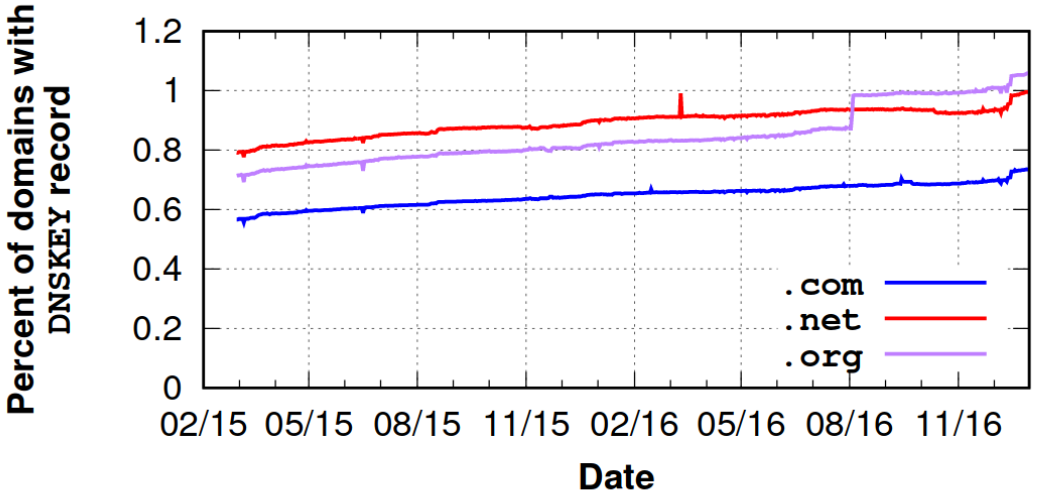


Figure 3: The percentage of all `.com`, `.org`, and `.net` second-level domains that have a `DNSKEY` record, from the Daily dataset. Between 0.75% and 1.0% of all domains publish a `DNSKEY` record at the time of writing.

Source (data from August 2016): https://securepki.org/sec17.html

Other enhancements

- DNSCrypt – signs DNS responses
- DNS over https

Other attacks

Cache poisoning

- Wrong responses can propagate
- They get cached potentially for long time (TTL in days)
- Example: leaving malicious network doesn’t clear cached domains

Turn off internet

- Internet doesn’t work without DNS
- DNS servers can be overloaded (DNS flood)

DNS amplification

- DNS replies 70x request size
- UDP - spoof source IP
- Result: overloaded target server

Domain owner privacy

- WHOIS – protocol to query the registered users or assignees of an Internet resource
- Interesting data is publicly available (name, address, e-mail address, phone number)

WHOIS

google.com

Updated 13 hours ago

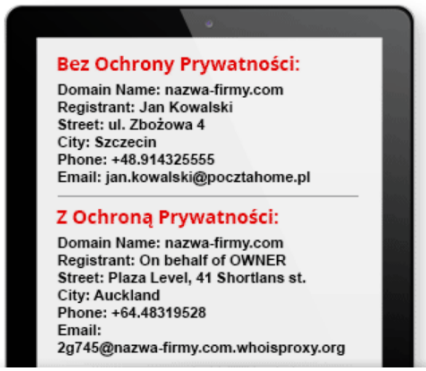
DOMAIN INFORMATION

Domain:	google.com
Registrar:	MarkMonitor Inc.
Registration Date:	1997-09-15
Expiration Date:	2020-09-13
Updated Date:	2018-02-21
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.google.com ns2.google.com ns3.google.com ns4.google.com

REGISTRANT CONTACT

Name:	Domain Administrator
Organization:	Google LLC
Street:	1600 Amphitheatre Parkway,
City:	Mountain View
State:	CA
Postal Code:	94043
Country:	US
Phone:	+1.6502530000
Fax:	+1.6502530001
Email:	dns-admin@google.com

Hiding information



Ochrona prywatności Twoich danych osobowych

Zadbaj już teraz o ochronę Twoich danych osobowych. Zdecyduj sam czy chcesz, aby Twoje imię i nazwisko, adres zamieszkania czy numer telefonu były widoczne w publicznej bazie domen WHOIS. Jeśli nie, zarejestruj domenę z ochroną danych.

Teraz ochrona prywatności Twoich danych osobowych w promocyjnej cenie **9,90 zł** netto/rok! (zamiast 50 zł netto/rok).

Zabezpiecz się przed:

- spamem
- kradzieżą tożsamości
- zewnętrznymi zagrożeniami

- Providing false info is bad idea
- Can pay extra to hide those details

Questions?