DNS Security

How it works ...

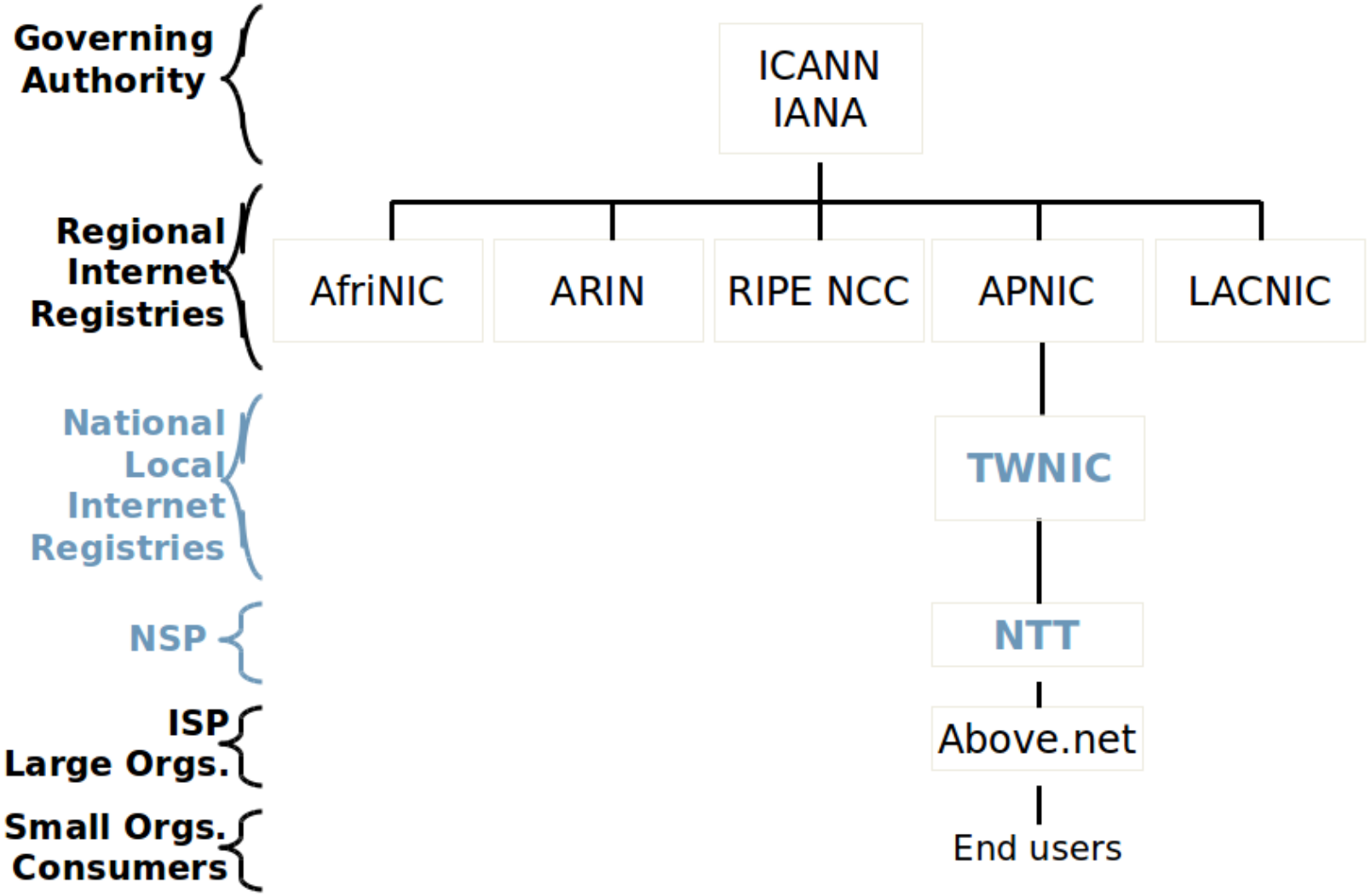
Internet Corporation for Assigned Names and Numbers (ICANN)
Nonprofit organization assigned to coordinate IANA's functions
Manages generic top-level domains (gTLDs) and country code top-level domains (ccTLDs)
Helps preserve the operational stability of the Internet
Achieves broad representation of global Internet community

Internet Assigned Numbers Authority (IANA)
Delegates local registrations of IP addresses to Regional Internet Registries
Administers the data in the root name servers, which is the top of the hierarchical DNS tree
Works with the Internet Engineering Task Force regarding parameters and protocols on the internet that registry related

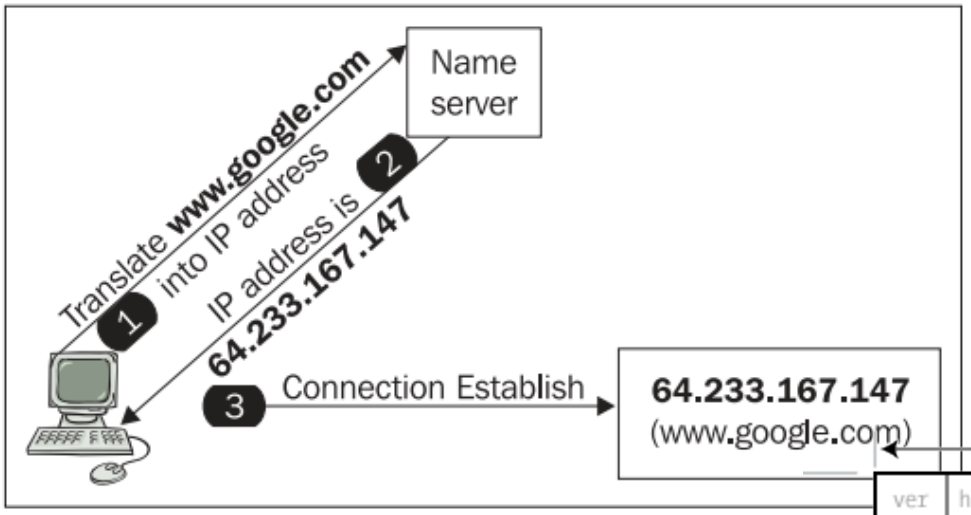
How it works ...

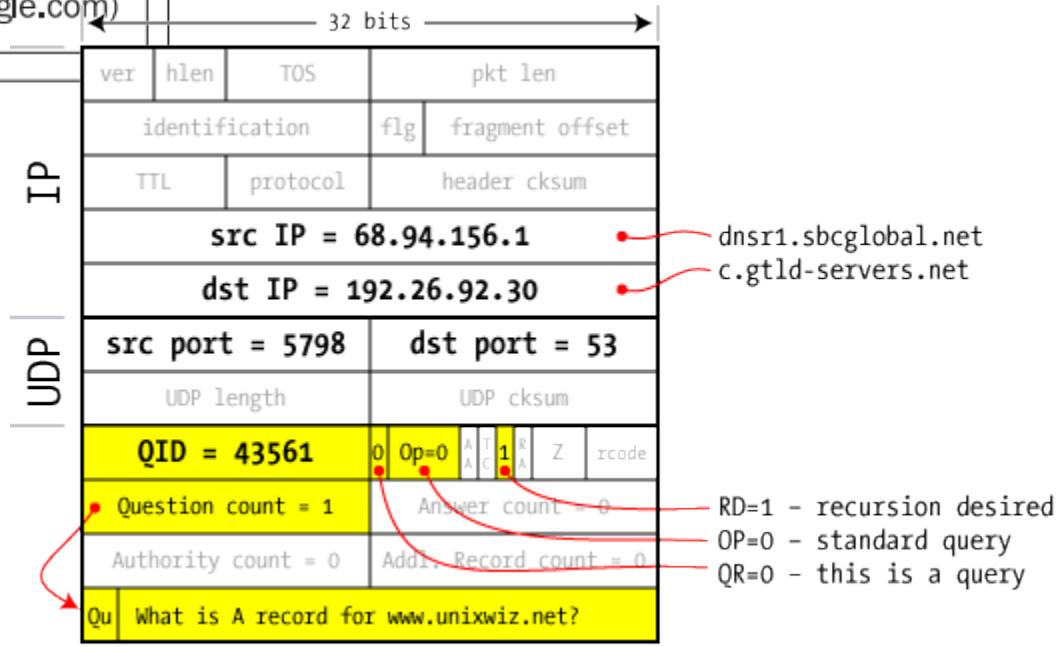
ARIN – American Registry for Internet Numbers
RIPE NCC – Réseaux IP Européens Network Coordination Centre
APNIC – Asia Pacific Network Information Centre
LACNIC – Latin America and Caribbean Internet Addresses Registry
AfriNIC – African Network Information Centre

How it works ...

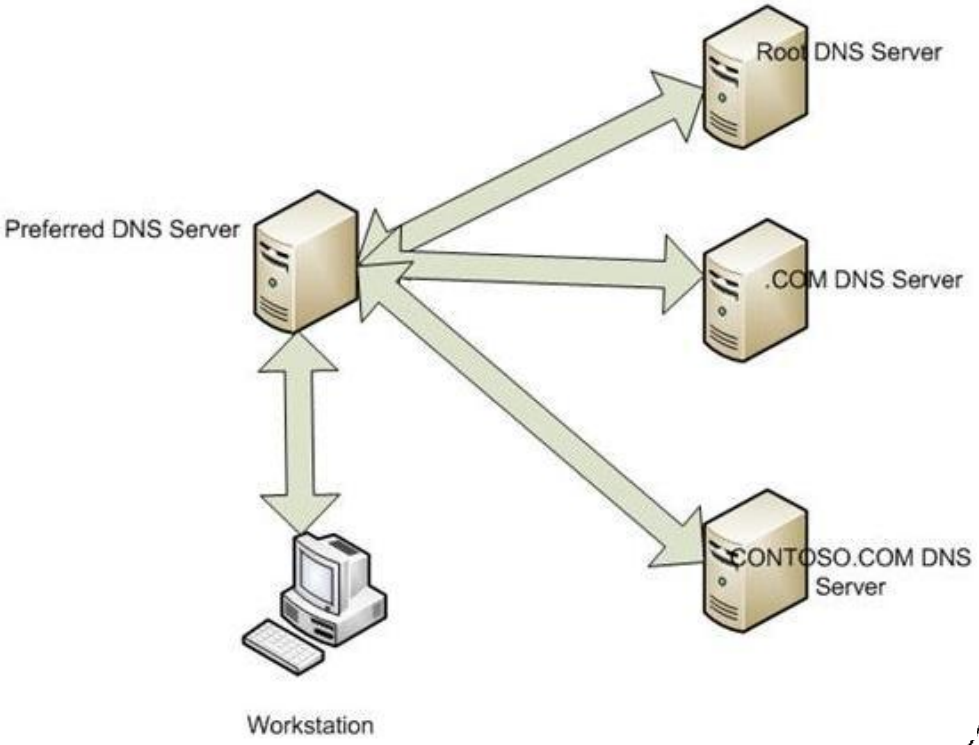

Governing Authority
Regional Internet Registries
National Local Internet Registries
NSP
ISP Large Orgs.
Small Orgs. Consumers
ICANN IANA
AfriNIC
ARIN
RIPE NCC
APNIC
LACNIC
TWNIC
NTT
Above.net
End users

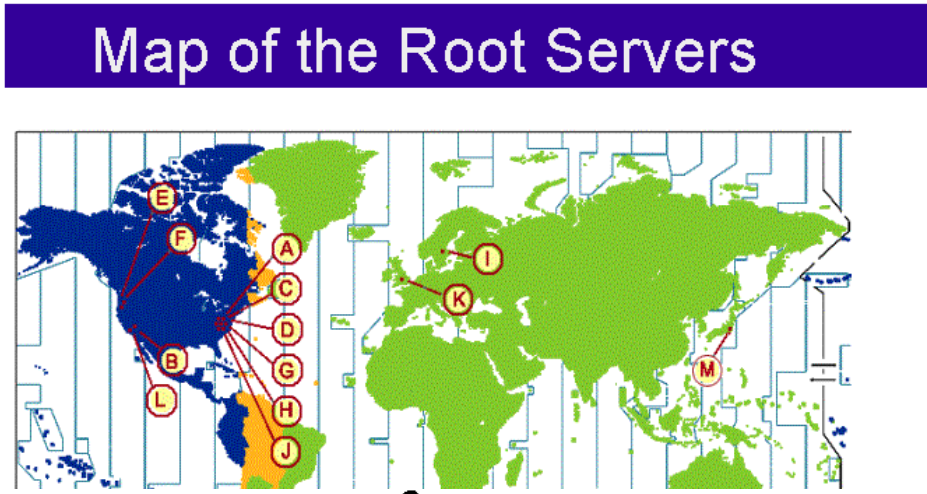
How it works ...

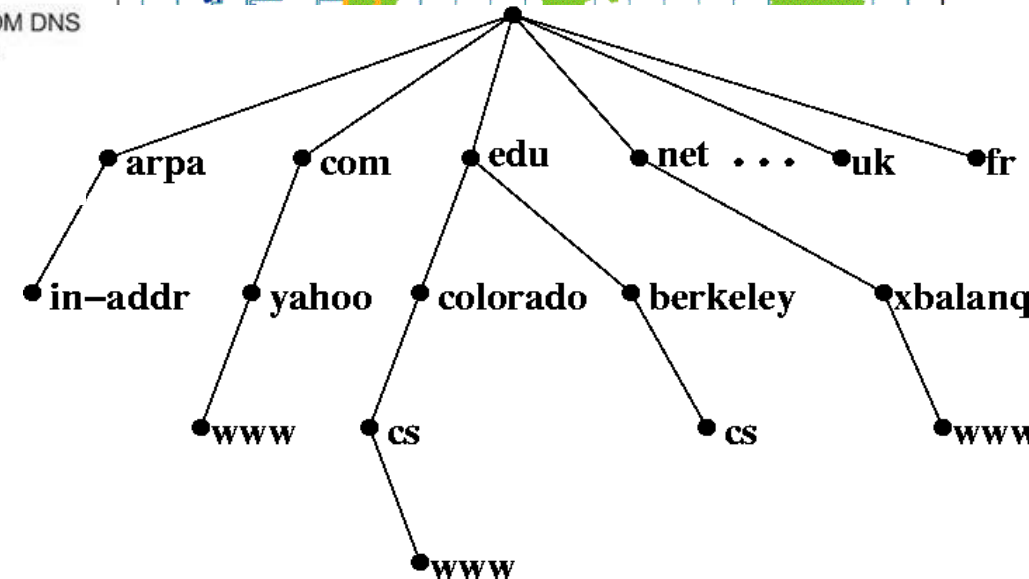

Name server
Translate www.google.com into IP address
1
2
IP address is 64.233.167.147
3
Connection Establish
64.233.167.147
(www.google.com)


32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 192.26.92.30
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43561
0
Op=0
1
Z
rcode
Question count = 1
Answer count = 0
Authority count = 0
Addl. Record count = 0
Qu
What is A record for www.unixwiz.net?
dnsr1.sbcglobal.net
c.gtld-servers.net
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

How it works ...


Root DNS Server
Preferred DNS Server
.COM DNS Server
CONTOSO.COM DNS Server
Workstation


Map of the Root Servers
E
F
A
C
D
G
H
J
B
L
I
K
M


arpa
com
edu
net . . .
uk
fr
in–addr
yahoo
colorado
berkeley
xbalanq
www
cs
cs
www
www

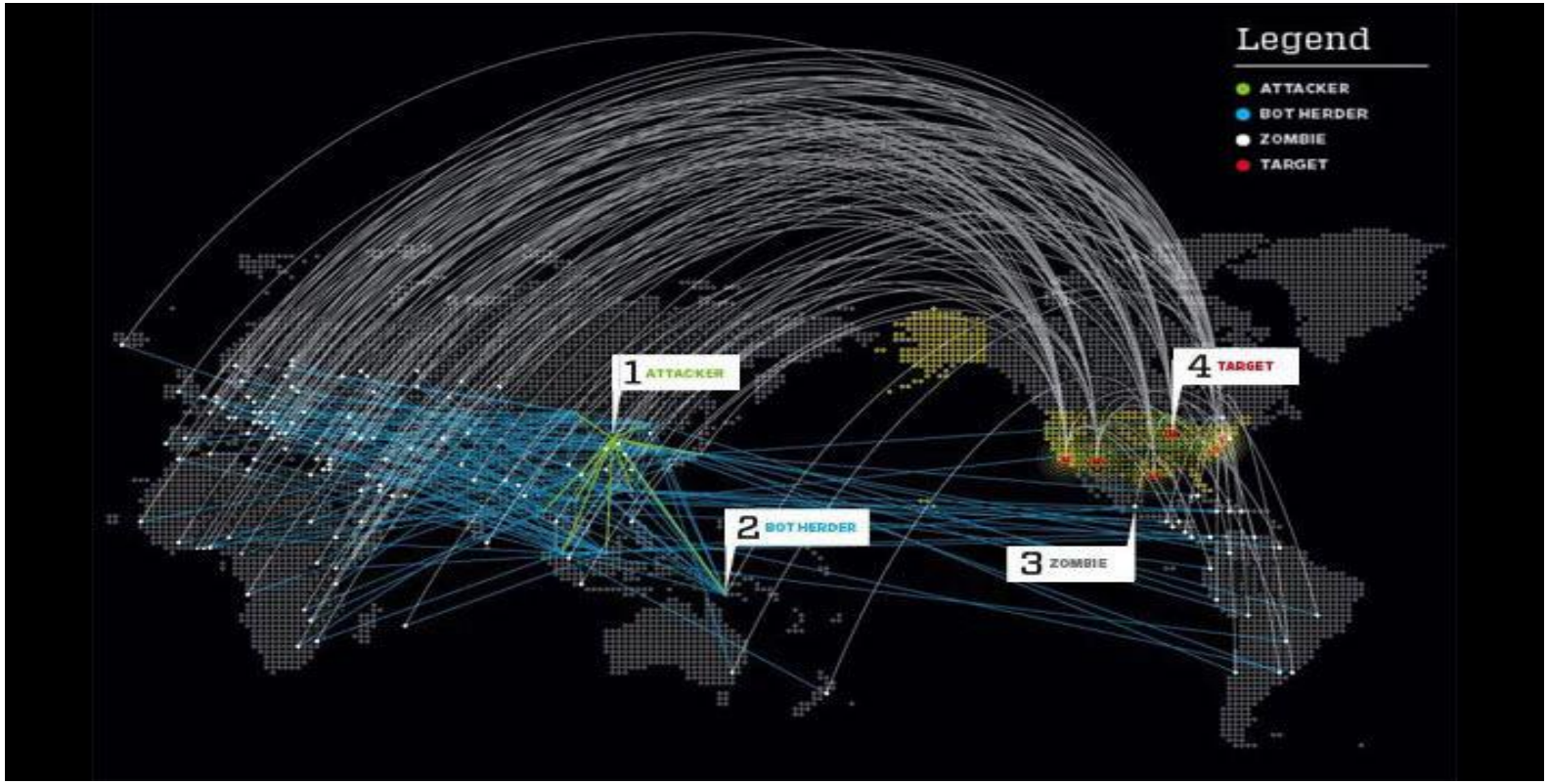
[Demo]

Use DNS for attacks

Giant Distributed System

Amplification attack

Fast-flux



Attacks ...

A. DNS: Server Attacks

B. DNS: Protocol Attacks
- DNS cache poisoning
- DNS Spoofing
- DNS ID Hacking

DNS Server Attacks

- Attacks taking advantage of bugs in DNS Software implementation (buffer overflows in BIND for instance).

- Attack by Denial of Service (using flooding).

DNS: Protocol Attacks

DNS cache poisoning:

attack consisting of making a DNS server cache false information: usually, a wrong record that will map a name to a "wrong" IP address.

Not always a hacker.

Cache Poisoning

Method 1:

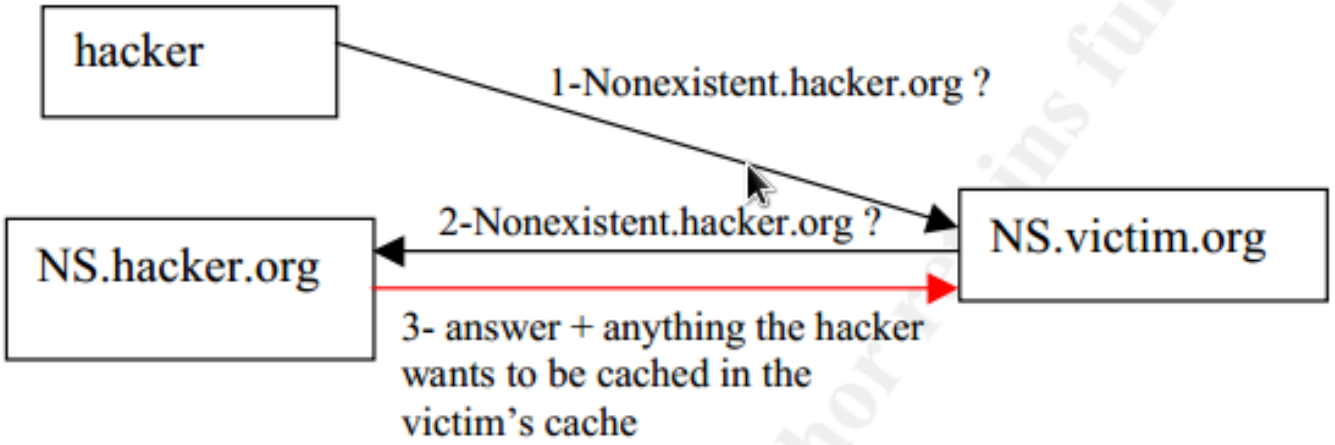
1. hacker asks the victim DNS for a nonexistent name mapping.

2. DNS, will go and ask the DNS server responsible for the required domain. Remember this server is under the control of the hacker.

3. The hacker will answer, and add in the answer anything he wants to be cached in the victim DNS' cache.

+ fixed in BIND, by forbidding anything that is not related to

the original request to be cached.

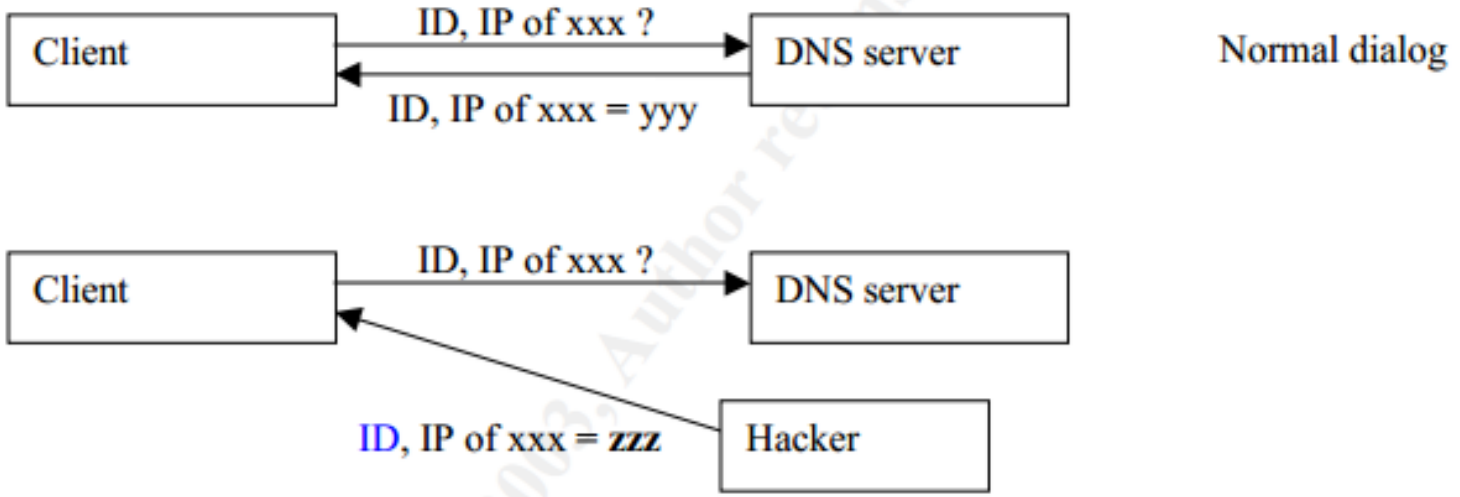


DNS: Protocol Attacks

DNS Spoofing:

answering a DNS request that was intended for another server (a “real” DNS server).

But DNS uses ID number to identifyqueries and answer, so the hacker needs to find the ID the client is waiting for: DNS ID hacking.



Defense

Randomized query ID:

- Attacker can make a LOT of queries with names that are not likely to exist in the cache

- Most of the attempts will fail, but one will eventually succeed

    In practice, apparently, it can succeed in as little as 10 seconds.

DNSSec

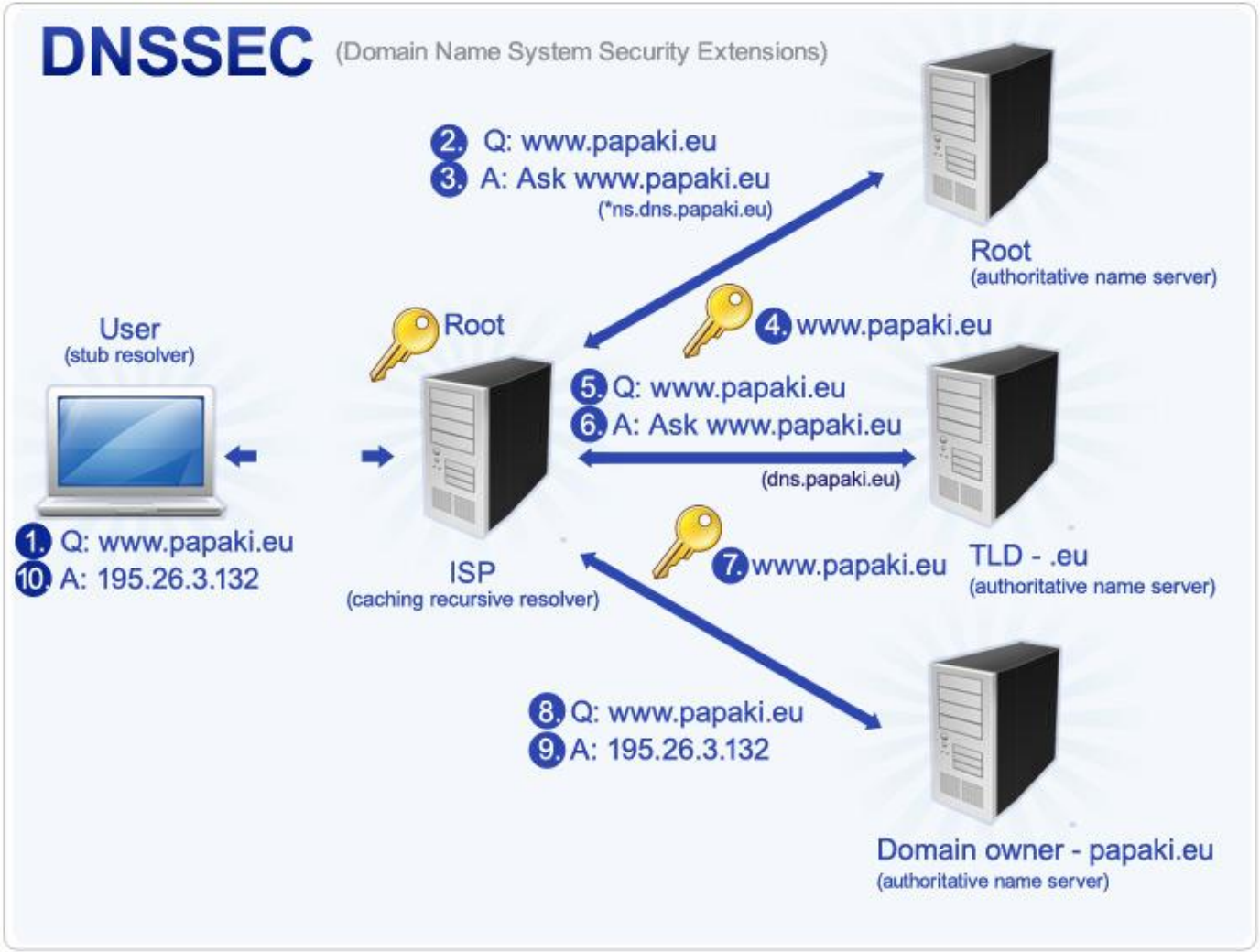
- Uses Chain-of-Trust to establish authenticity

– Each child signs their zone “resource record set”with the private key

– Child’s public-key authenticity is established by the parent. Whose key is verified by it’s parent and so-on until we reach the root

- Can co-exist with existing DNS infrastructure

DNSSec


DNSSEC
(Domain Name System Security Extensions)
2. Q: www.papaki.eu
3. A: Ask www.papaki.eu
(*ns.dns.papaki.eu)
Root
(authoritative name server)
User
(stub resolver)
Root
4. www.papaki.eu
5. Q: www.papaki.eu
6. A: Ask www.papaki.eu
(dns.papaki.eu)
1. Q: www.papaki.eu
10. A: 195.26.3.132
ISP
(caching recursive resolver)
7. www.papaki.eu
TLD - .eu
(authoritative name server)
8. Q: www.papaki.eu
9. A: 195.26.3.132
Domain owner - papaki.eu
(authoritative name server)

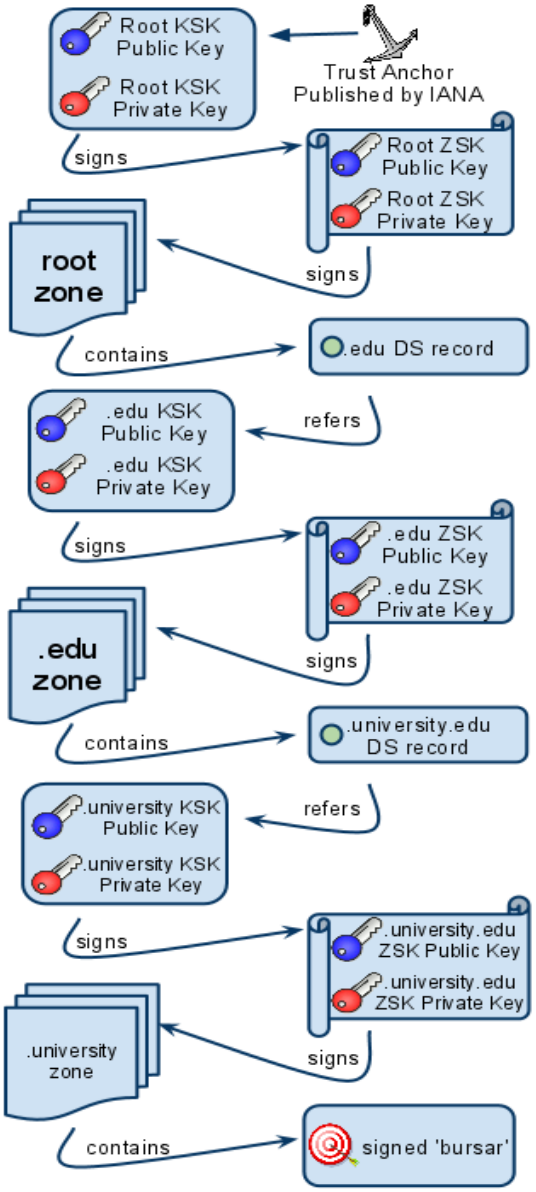
DNSSec

Chain Of Trust

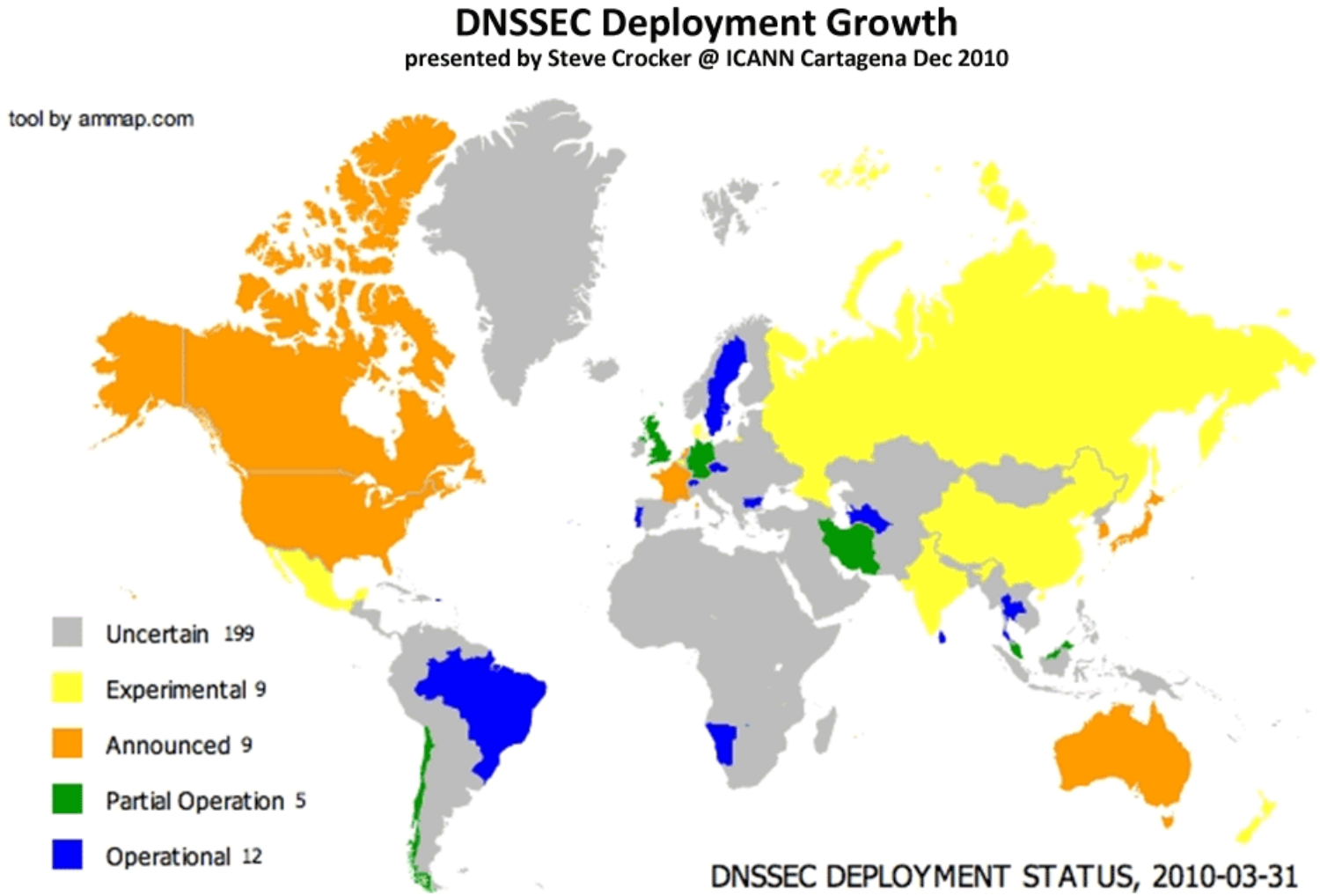
KSK: Key Signing Key

ZSK: Zone Signing Key

DS: Delegated Signer



DNSSec



(The information above is representative of limited publicly available data only. The deployment of DNSSEC is rapidly changing in the market and this data should not be taken as authoritative.)