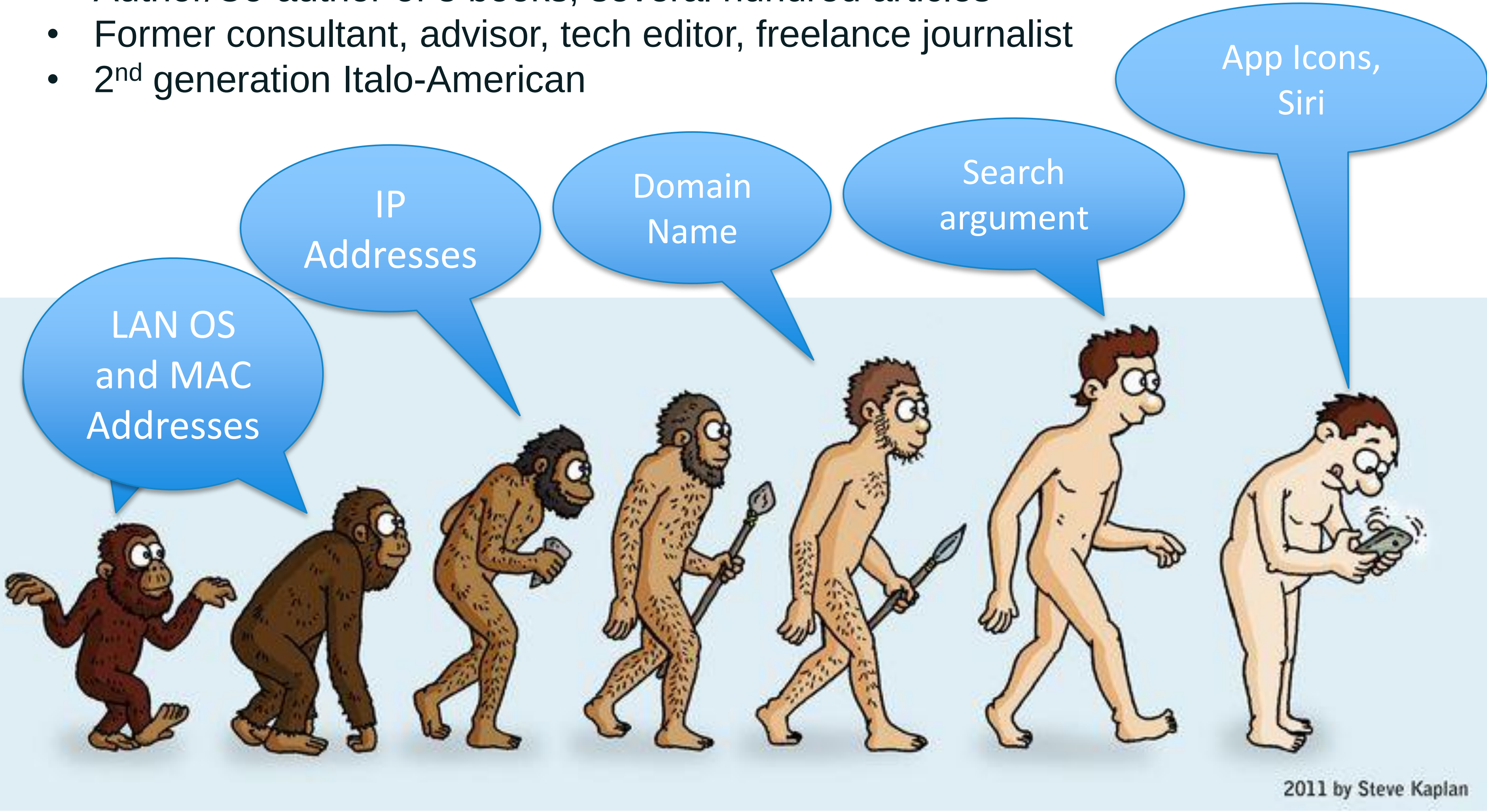
Attacks against the DNS

Dave Piscitello
VP Security and ICT Coordination
April 2015
dave.piscitello@icann.org

ICANN

About Dave

- Involved in networking and Internet since 1977
- Member of Internet Engineering Steering Group
- Author/Co-author of 6 Internet RFCs
- Author/Co-author of 3 books, several hundred articles
- Former consultant, advisor, tech editor, freelance journalist
- 2nd generation Italo-American



2011 by Steve Kaplan

Agenda

- How does the DNS work?
- Attacking the DNS
- Attack mitigations and countermeasures

Part 1

- How does the DNS work?
- Attacking the DNS
- Attack mitigations and countermeasures

What is the Domain Name System?

A distributed database primarily used to obtain

the IP address, a number, e.g.,
192.168.23.1 or fe80::226:bbff:fe11:5b32

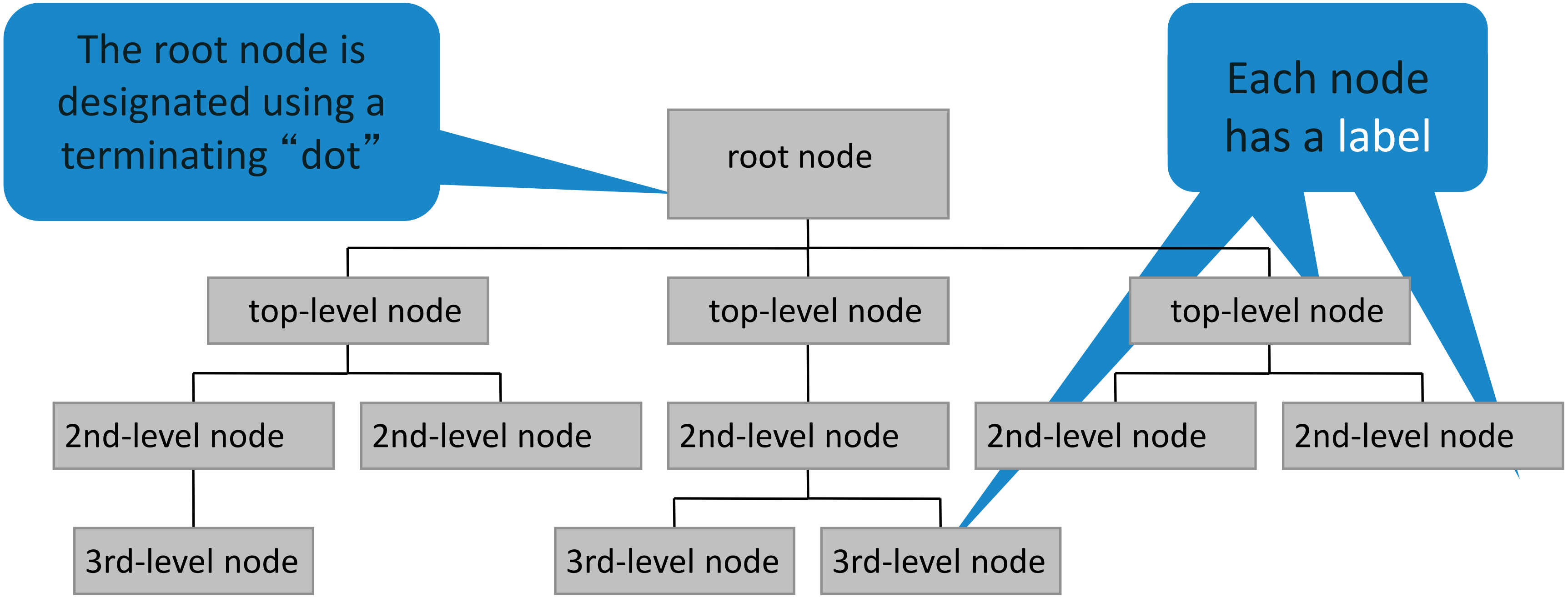
that is associated with a

user-friendly name (www.example.com)

Why do we need a DNS?
It's hard to remember lots of four decimal numbers
and it's impossibly hard to remember hexadecimal ones

Structure of the Distributed DNS Database

The formal structure of the DNS database is
an inverted tree with the root node at the top

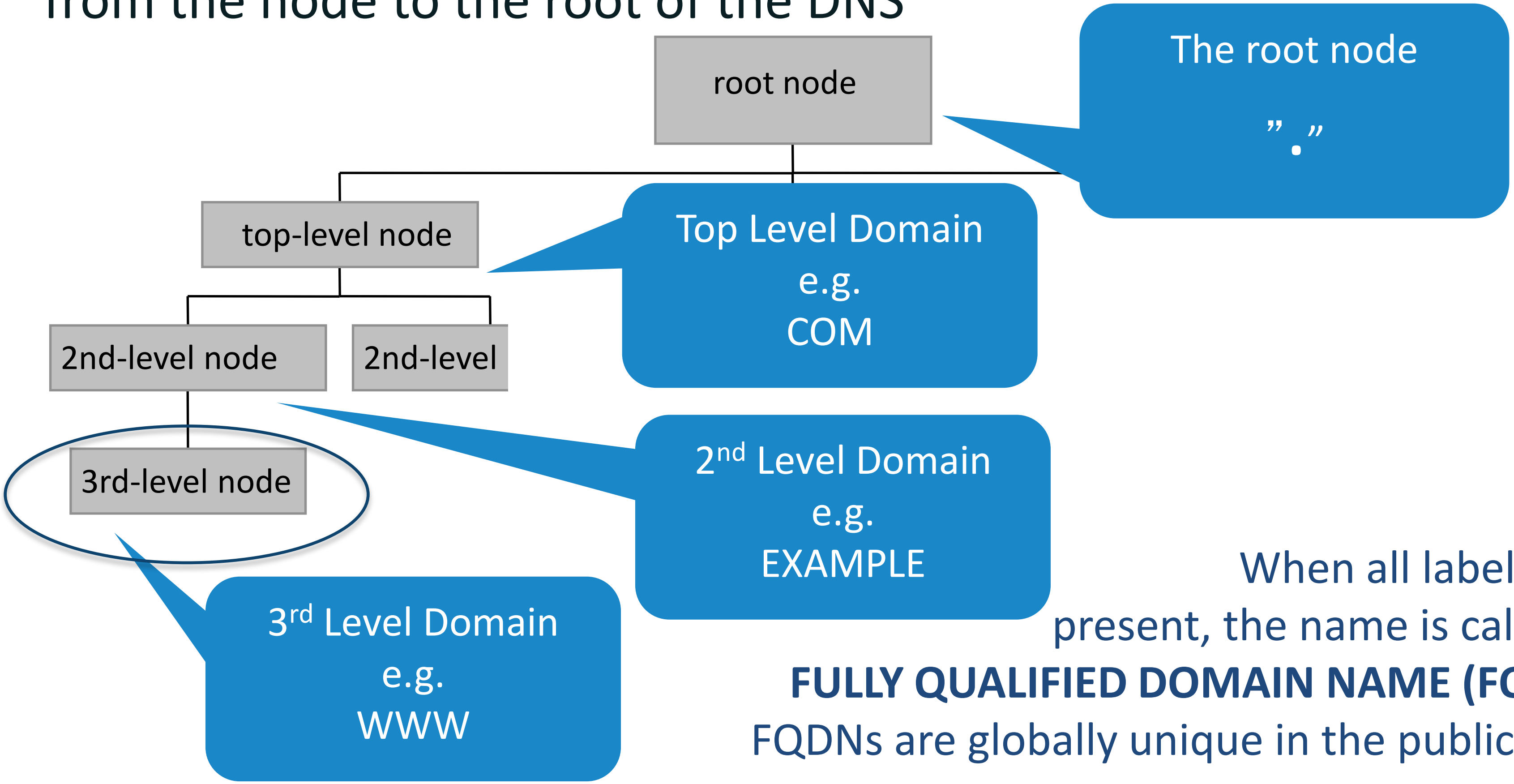


The DNS is *a* public name space.
It is one of *many* name spaces used on the Internet.

Labels and Domain Names

Each node in the DNS name space has a label

The domain name of a node is a *list* of the labels on the path from the node to the root of the DNS



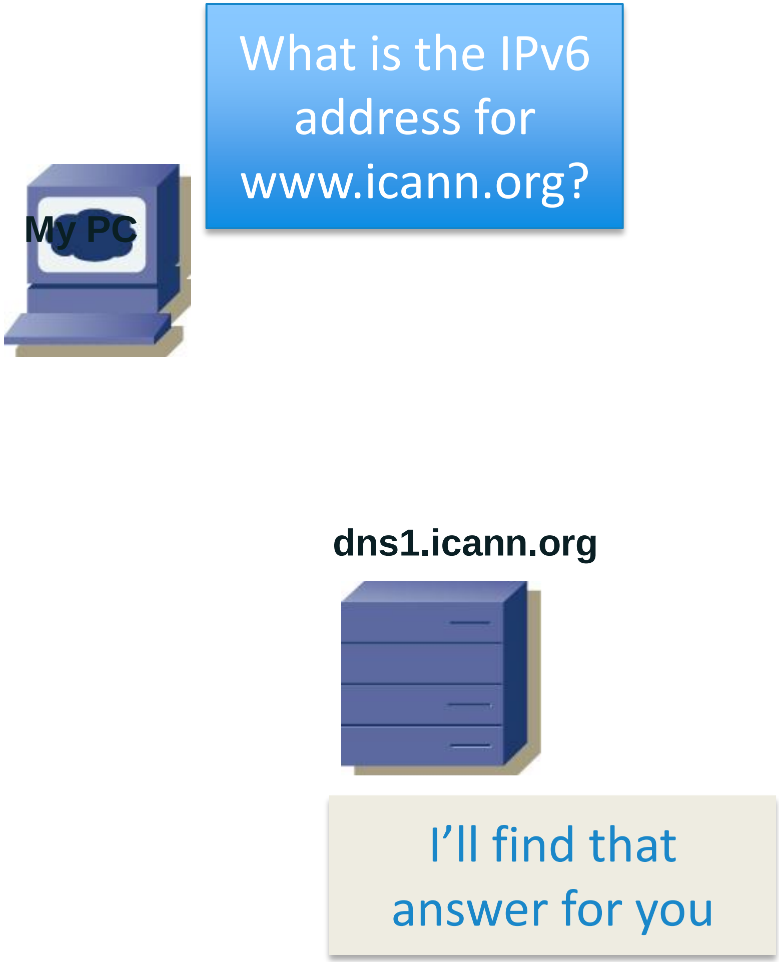
When all labels are present, the name is called a **FULLY QUALIFIED DOMAIN NAME (FQDN)**
FQDNs are globally unique in the public DNS

Operational elements of the DNS

- Authoritative Name Servers host zone data
  - The set of “DNS data” that the registrant publishes
- Recursive Name Resolvers (“resolvers”)
  - Systems that find answers to queries for DNS data
- Caching resolvers
  - Recursive resolvers that find and store answers locally for “TTL” period of time
- Client or “stub” resolvers
  - Software in applications, mobile apps or operating systems that query the DNS and process responses
  - Small business or home access routers may have stubs, too!

DNS: Internet’s directory assistance

- Client “stub” resolvers ask questions
  - Software in applications, mobile apps or operating systems that issue DNS queries and process responses
- Recursive name resolvers find answers to queries for DNS data



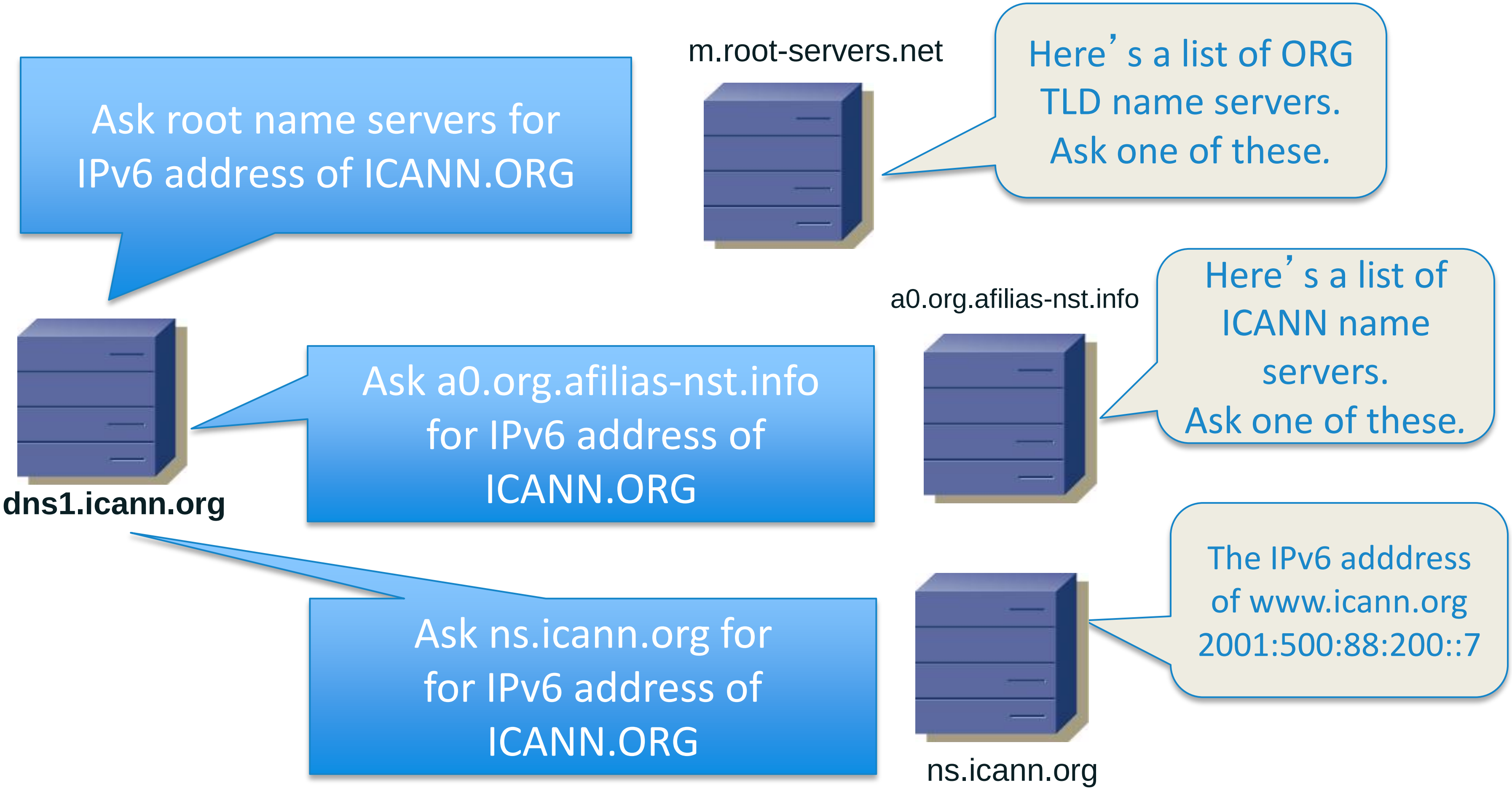
What is the IPv6 address for www.icann.org?

I’ll find that answer for you

Domain name “directory assistance”

How does a resolver find the IP address of ICANN.ORG?

- Resolvers find answers by asking questions *iteratively*



Ask root name servers for IPv6 address of ICANN.ORG

m.root-servers.net

Here’ s a list of ORG TLD name servers. Ask one of these.

dns1.icann.org

Ask a0.org.afilias-nst.info for IPv6 address of ICANN.ORG

a0.org.afilias-nst.info

Here’ s a list of ICANN name servers. Ask one of these.

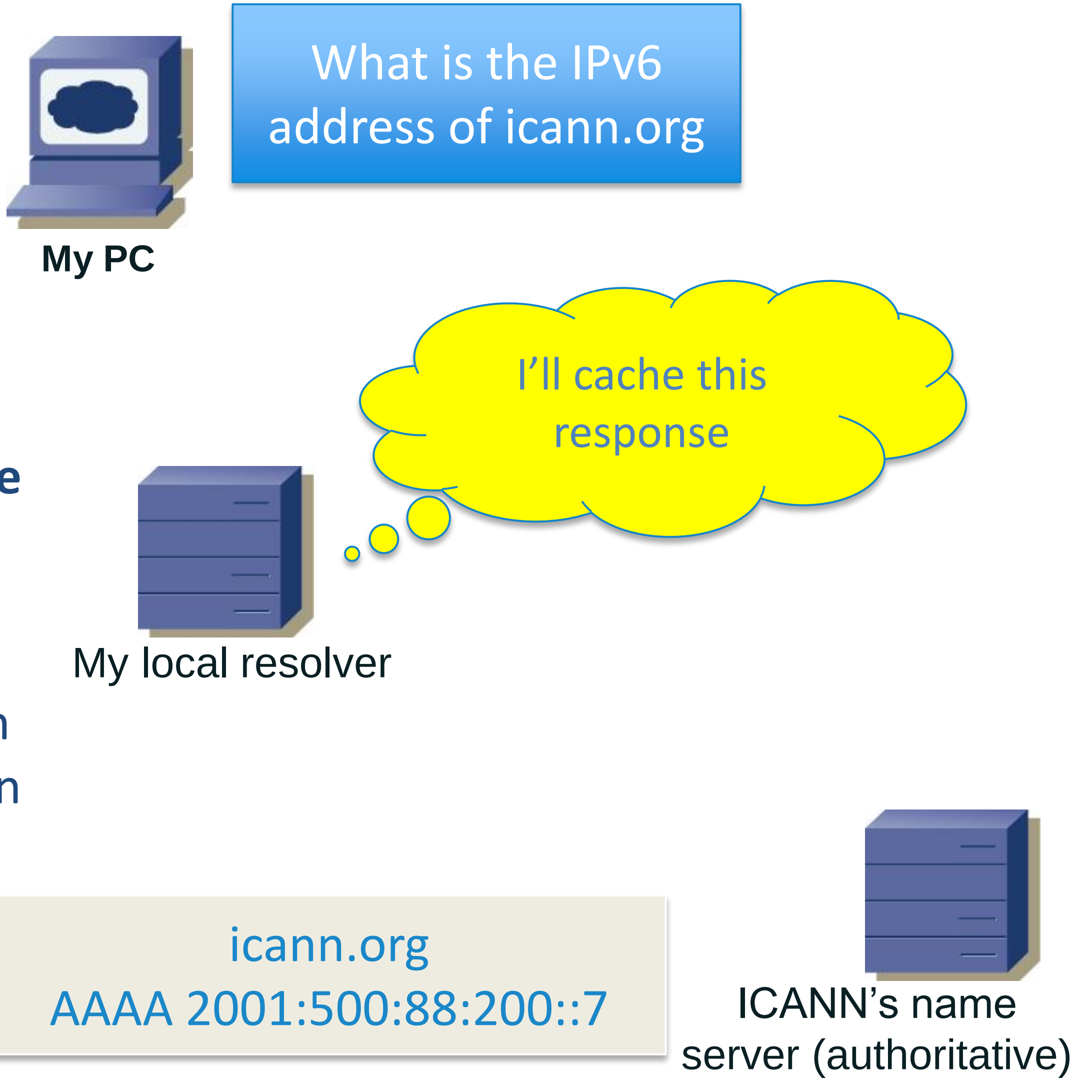
Ask ns.icann.org for for IPv6 address of ICANN.ORG

ns.icann.org

The IPv6 adddress of www.icann.org 2001:500:88:200::7

What is caching?

- Resolvers may *cache* DNS records they receive from other name servers as they process client queries
  - Speeds up resolution
  - Saves bandwidth
  - Responses are **non-authoritative**
- Are cached records valid forever?
  - No. The time to live (TTL) field in DNS records bounds how long an iterative resolver can cache that particular record



My PC

What is the IPv6 address of icann.org

I'll cache this response

My local resolver

icann.org
AAAA 2001:500:88:200::7

ICANN's name server (authoritative)

Summary

1 The DNS is a public, distributed database

2 The DNS allows us to use names rather than numbers to navigate the Internet

3 The operational elements of the DNS span from critical infrastructure to user devices

Agenda

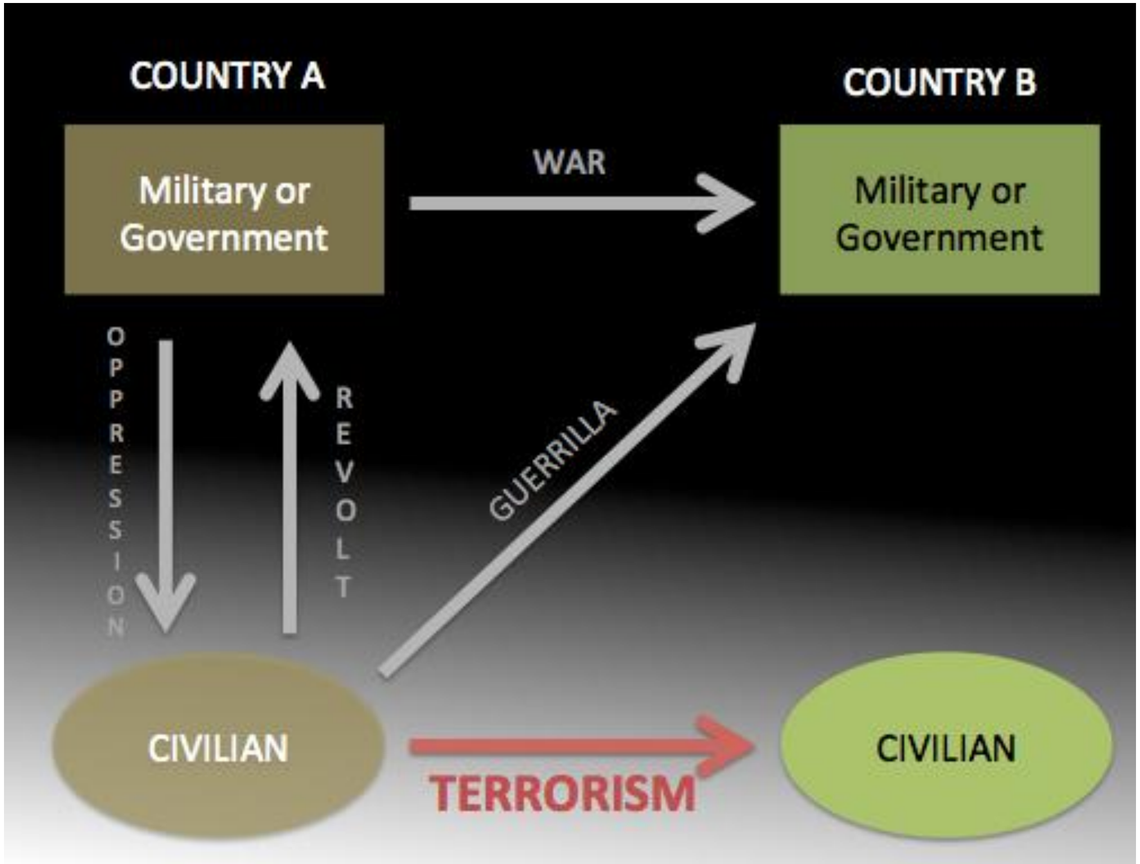
- How does the DNS work?
- Attacking the DNS
- Attack mitigations and countermeasures

What can I do with a domain name?

- An engineer’s answer
  - Assign user friendly names to a computer (server) that hosts *Internet applications:*
  - Web, blog, file server, email, IP telephony
- A businessman’s answer
  - Create a merchant or other commercial online presence
  - Join a commodities market: buy, sell, auction domain names
  - Run a commercial service
- A government official’s answer
  - Provide services for public interest
- A criminal’s, insurgent’s, or terrorist’s answer
  - Misuse, exploit or disrupt public or business services

Motives to Attack or Exploit the DNS

Actor have specific motives or incentives to attack critical cyber infrastructures, including DNS



Where are cybercrime and espionage in this diagram?

DNS Attack landscape

Target	Authoritative Name Server	Recursive Resolver	Stub Resolver
Access bandwidth	✔	✔	✔
Access network elements	✔	✔	✔
NS or device:			
Hardware	✔	✔	✔
OS software	✔	✔	✔
Name server software	✔	✔	
Cache		✔	✔
Application software			✔
Administration	✔	✔	✔
Configuration	✔	✔	✔

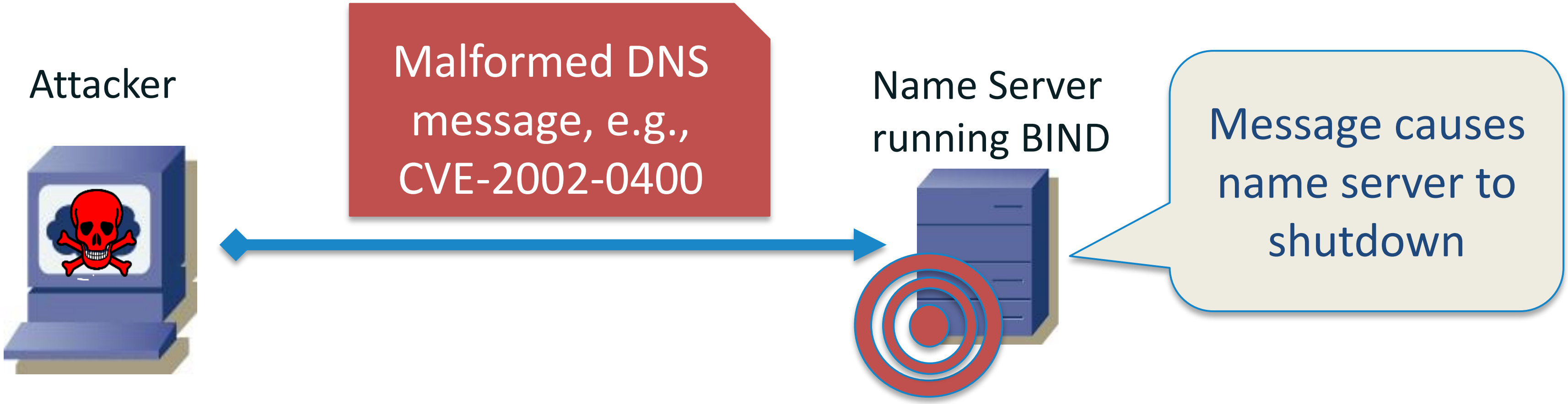
Attacks against name servers or recursors

- “Exploit to fail” Denial of Service (DOS) attack
- “Exploit to own” DOS attack
- Reflection attack
- Amplification attack
- Distributed DOS attack
- Cache Poisoning or Exhaustion attacks
- Reconnaissance attacks

Let’s look at some examples

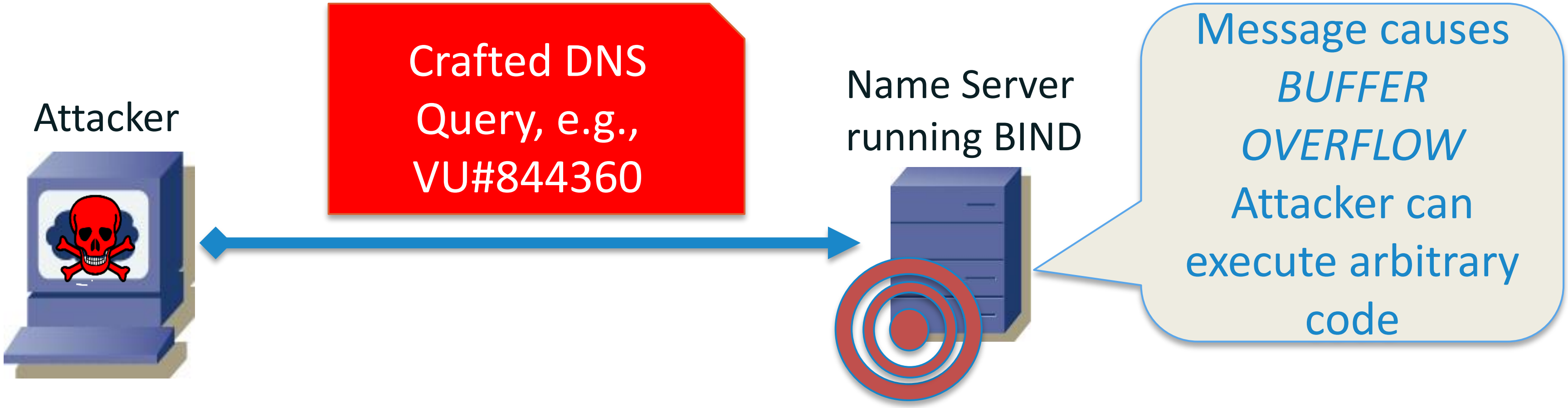
"Exploit to fail" DOS attack

- Exploit a vulnerability in some element of a name server infrastructure to cause interruption of name resolution service
- Example: Malicious DNS message injection
  - http://www.cvedetails.com/cve/CVE-2002-0400/

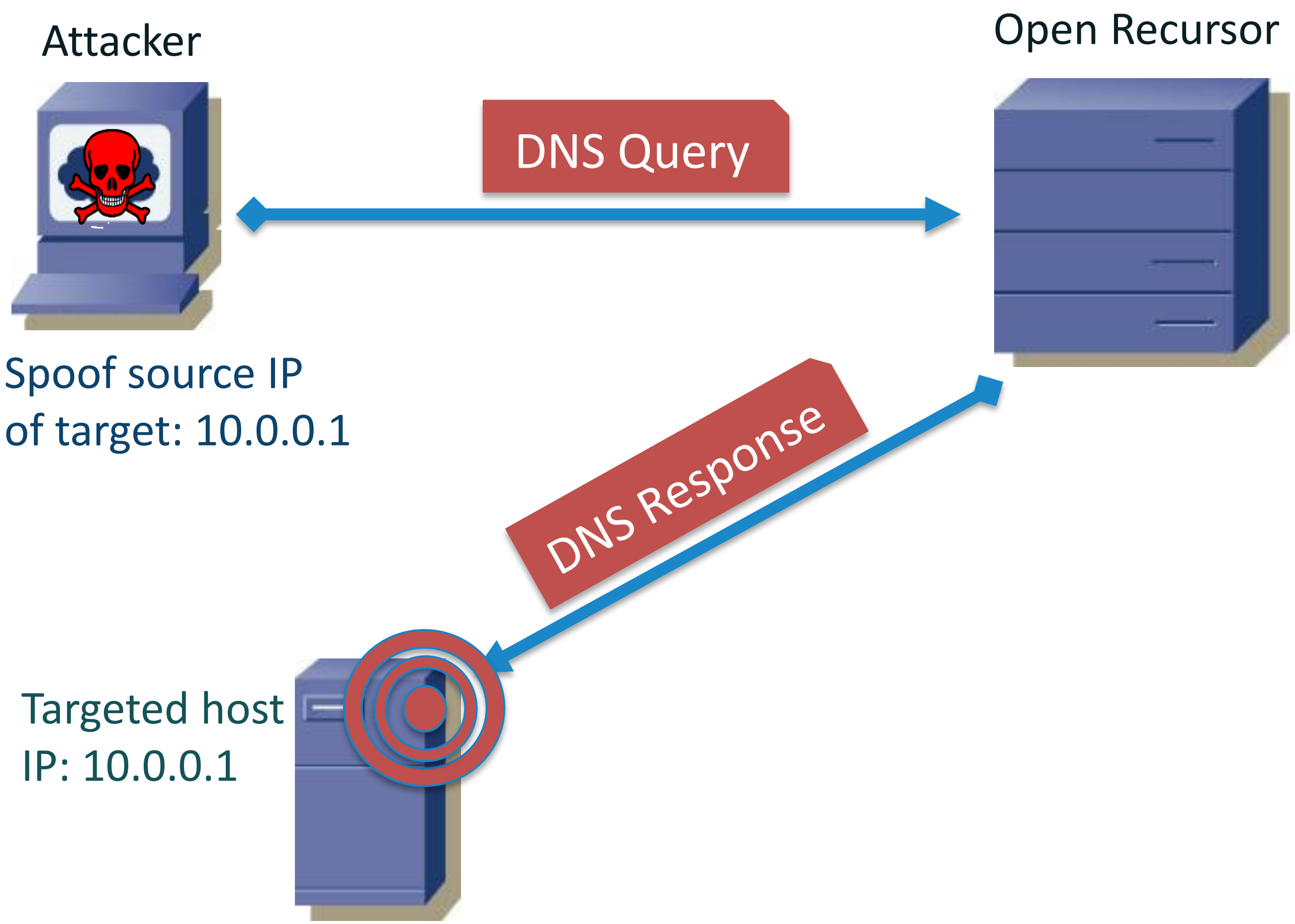

Attacker
Malformed DNS message, e.g., CVE-2002-0400
Name Server running BIND
Message causes name server to shutdown

“Exploit to own” DOS attack

- Exploit a vulnerability in some element of a name server infrastructure to gain system administrative privileges
- Example: Arbitrary/remote code execution
    - http://www.kb.cert.org/vuls/id/844360

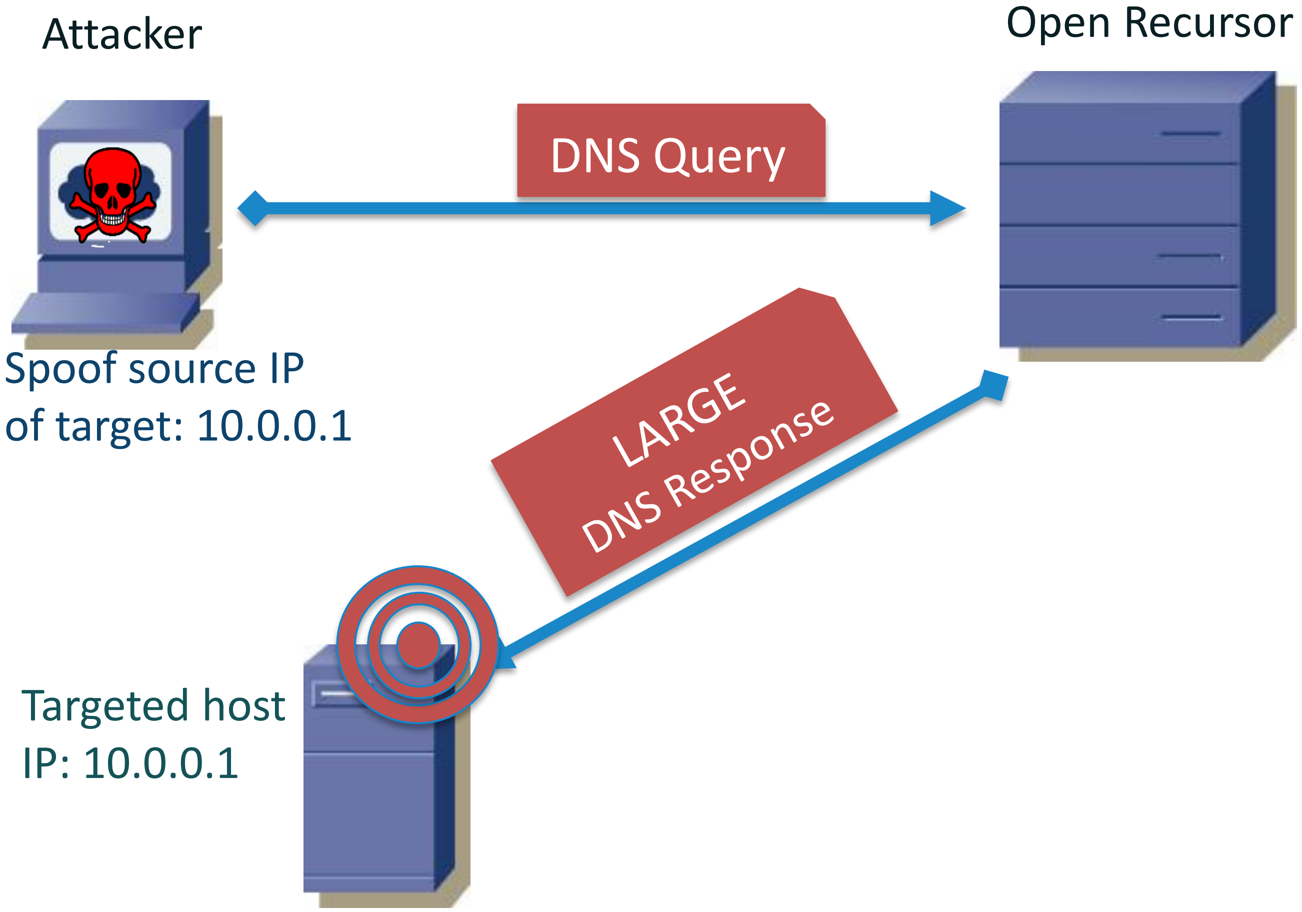

Attacker
Crafted DNS Query, e.g., VU#844360
Name Server running BIND
Message causes *BUFFER OVERFLOW* Attacker can execute arbitrary code

Reflection attack



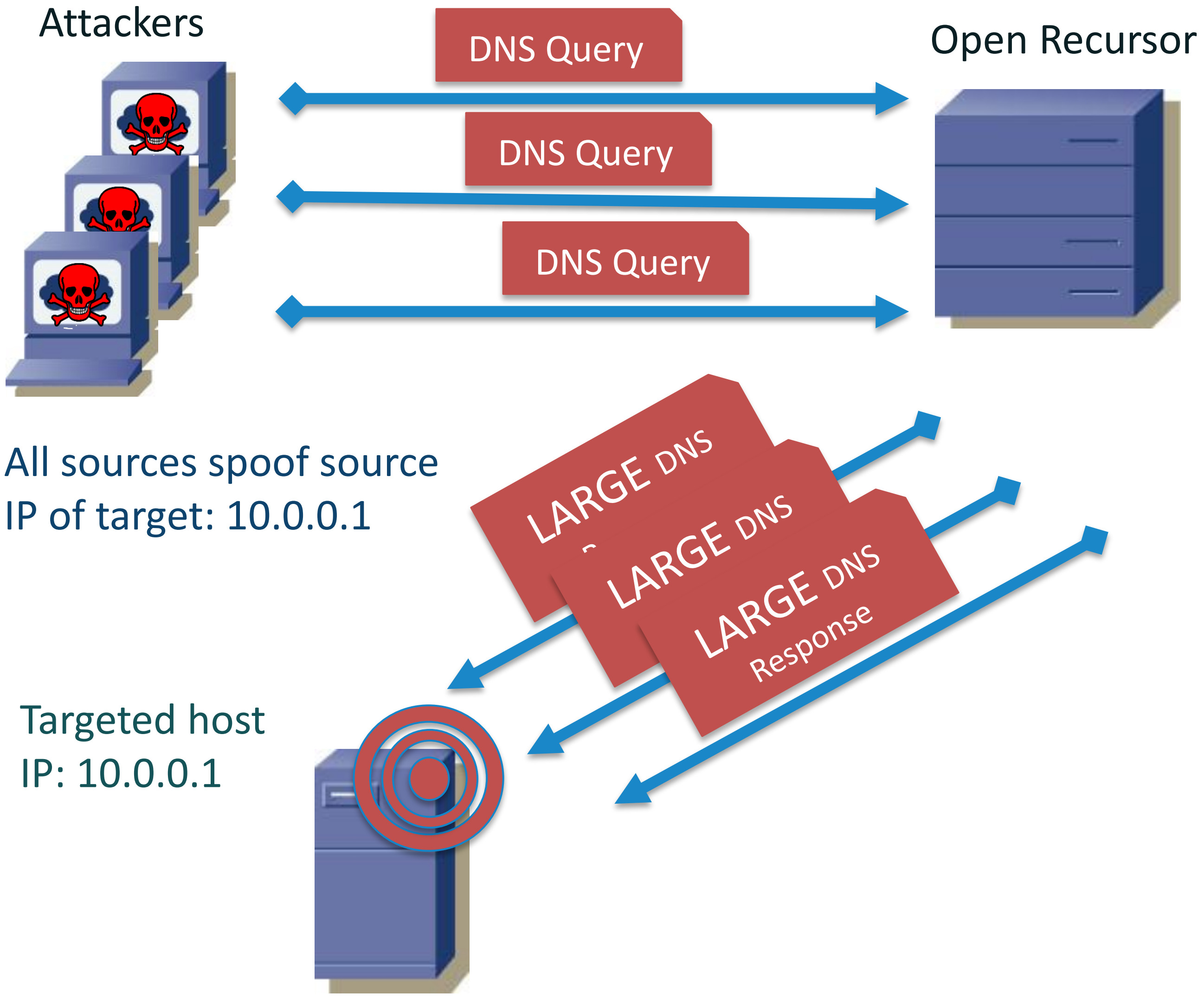
- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends response to targeted host
- Response delivered to targeted host

Reflection and Amplification attack



- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends LARGE responses to targeted host
- *Amplified* responses delivered to targeted host consume resources faster

Distributed reflection and amplification attack (DDoS)



Attackers

DNS Query

DNS Query

DNS Query

Open Recursor

All sources spoof source
IP of target: 10.0.0.1

LARGE DNS

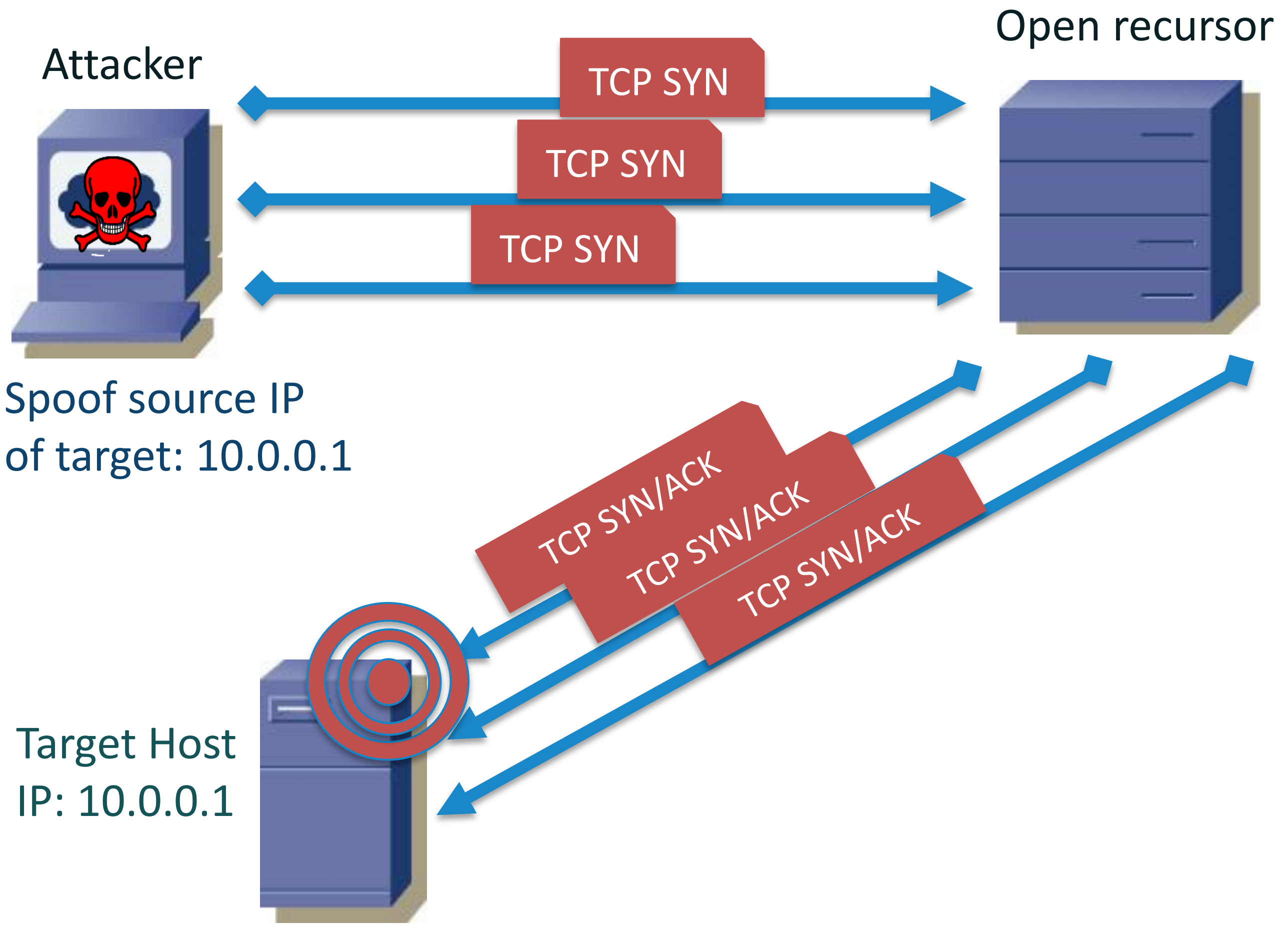
LARGE DNS

LARGE DNS
Response

Targeted host
IP: 10.0.0.1

- Launch reflection and amplification attack from 1000s of origins
- Reflect through open recursor
- Deliver 1000s of large responses to target

Resource depletion DOS attack

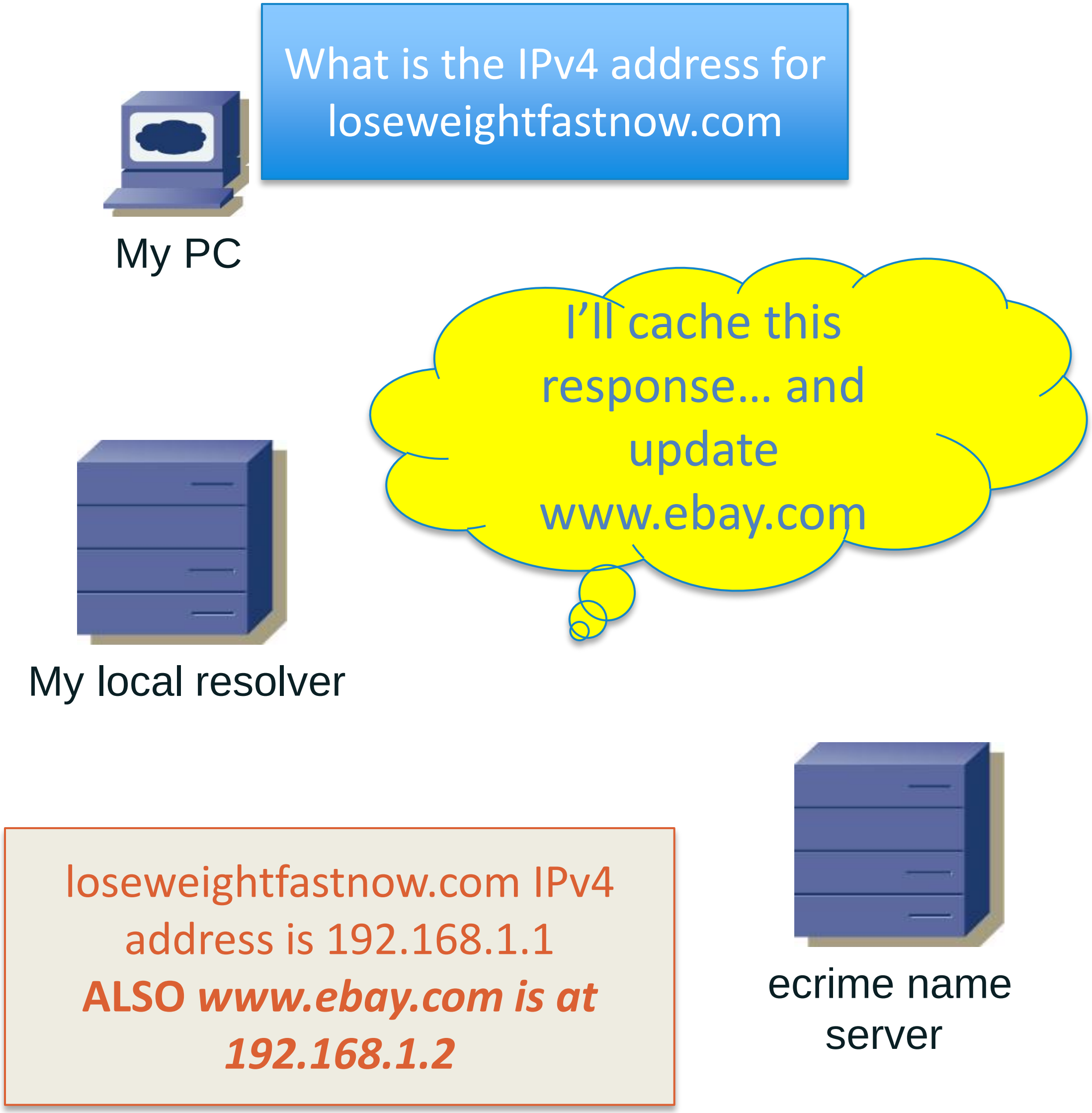


- Attacker sends flood of DNS messages over TCP from spoofed IP address of target
- Name server allocates resources for connections until resources are exhausted
- Name resolution is degraded or interrupted

Basic Cache Poisoning

Attacker

- Launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry



What is the IPv4 address for loseweightfastnow.com

My PC

I'll cache this response... and update www.ebay.com

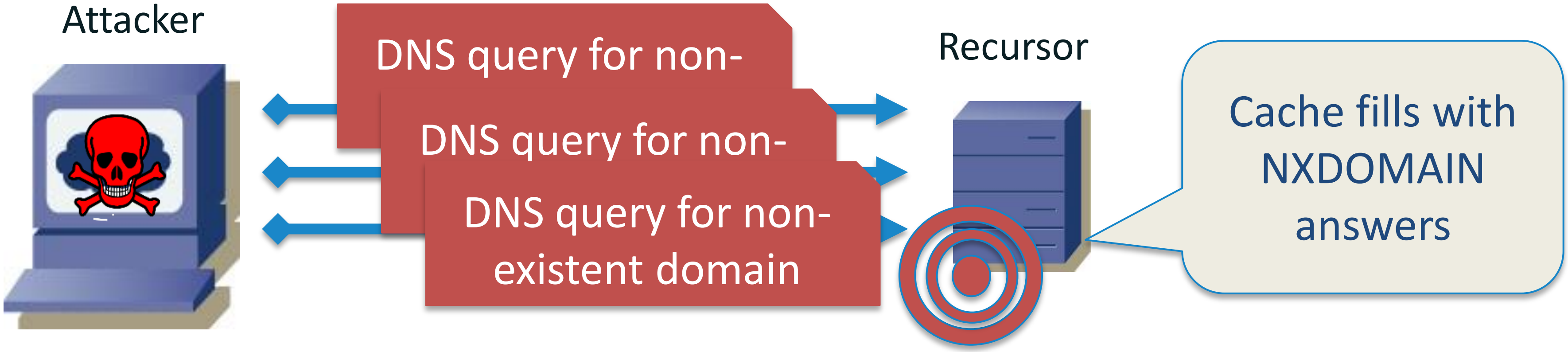
My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

NXDOMAIN Cache Exhaustion

- Attacker floods recursor with DNS queries for non-existent domain names
- Recursor attempts to resolve queries and adds each NXDOMAIN answer to cache
- Recursor’s cache fills with useless answers
- Processing of legitimate DNS queries is degraded


Attacker
DNS query for non-
DNS query for non-
DNS query for non-existent domain
Recursor
Cache fills with NXDOMAIN answers

Phantom Domain Attack has similar effects

TTL Bypass Attack (Kaminski)

- Query “sibling” names via targeted recursor
  - 1.example.com, 2.example.com, 2.example.com…
  - These are not likely to be cached so there’s a 1/65536 chance of guessing the correct transaction ID
- Impersonate the authoritative name server
- Answer the sibling whose transaction ID you guessed
- Also provide answer for www.example.com
- You’re spoofing the authoritative DNS so recursors will accept this new address for www.example.com in your answer for the sibling name

Reconnaissance Attacks

- Zone Transfer
  - – Query DNS to obtain list of domain's name servers
  - – Impersonate a secondary name server from list
  - – Ask primary for zone
- Zone Enumeration, a.k.a.,
  - – Use DNSSEC NSEC records to "zone walk"
  - – Use a "dictionary" of subdomain labels to get partial name space and topology information

These precursor attacks provide intelligence for subsequent attacks

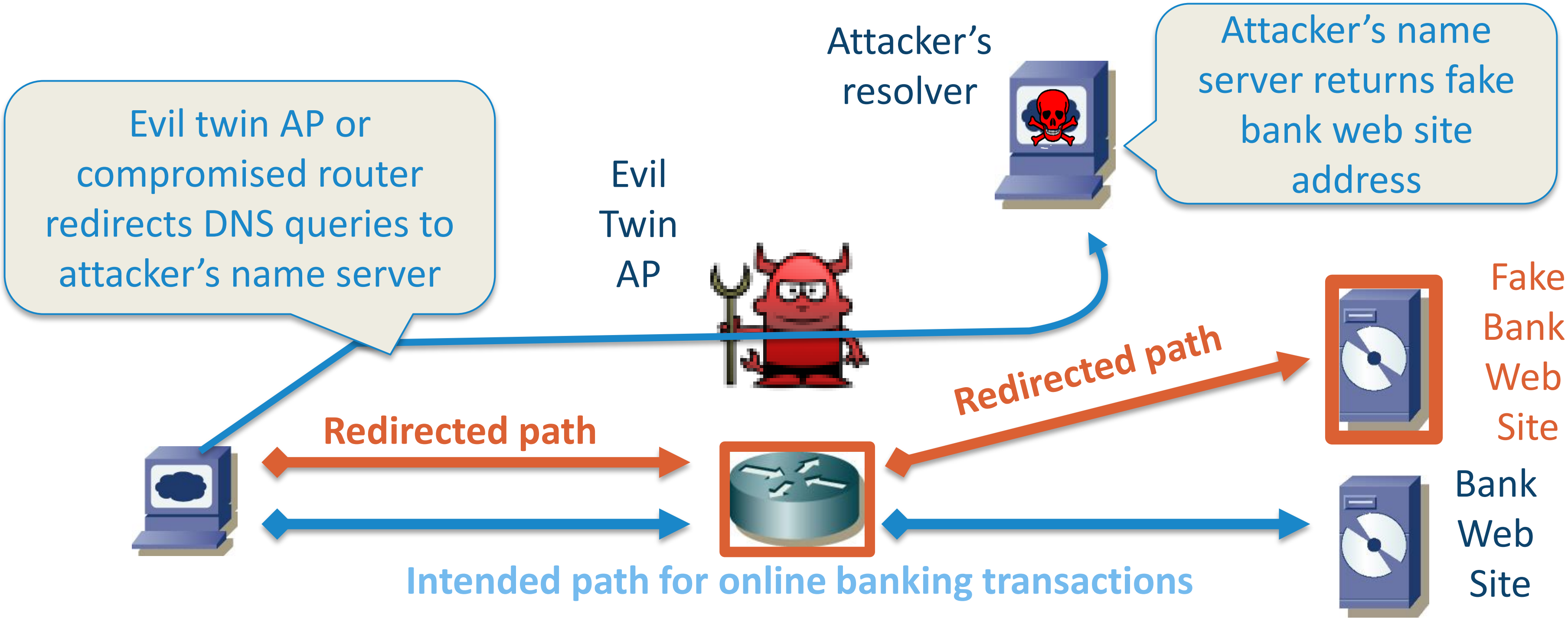
Attacks against stub resolvers

- Query interception attack
- DNS Response modification
  - – Also called Name Error resolution
- Configuration poisoning attack
- DNS hostname overflow attack

Let's look at some examples

Query Interception (DNS Hijacking)

- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point



Evil twin AP or compromised router redirects DNS queries to attacker's name server

Evil Twin AP

Attacker's resolver

Attacker's name server returns fake bank web site address

Fake Bank Web Site

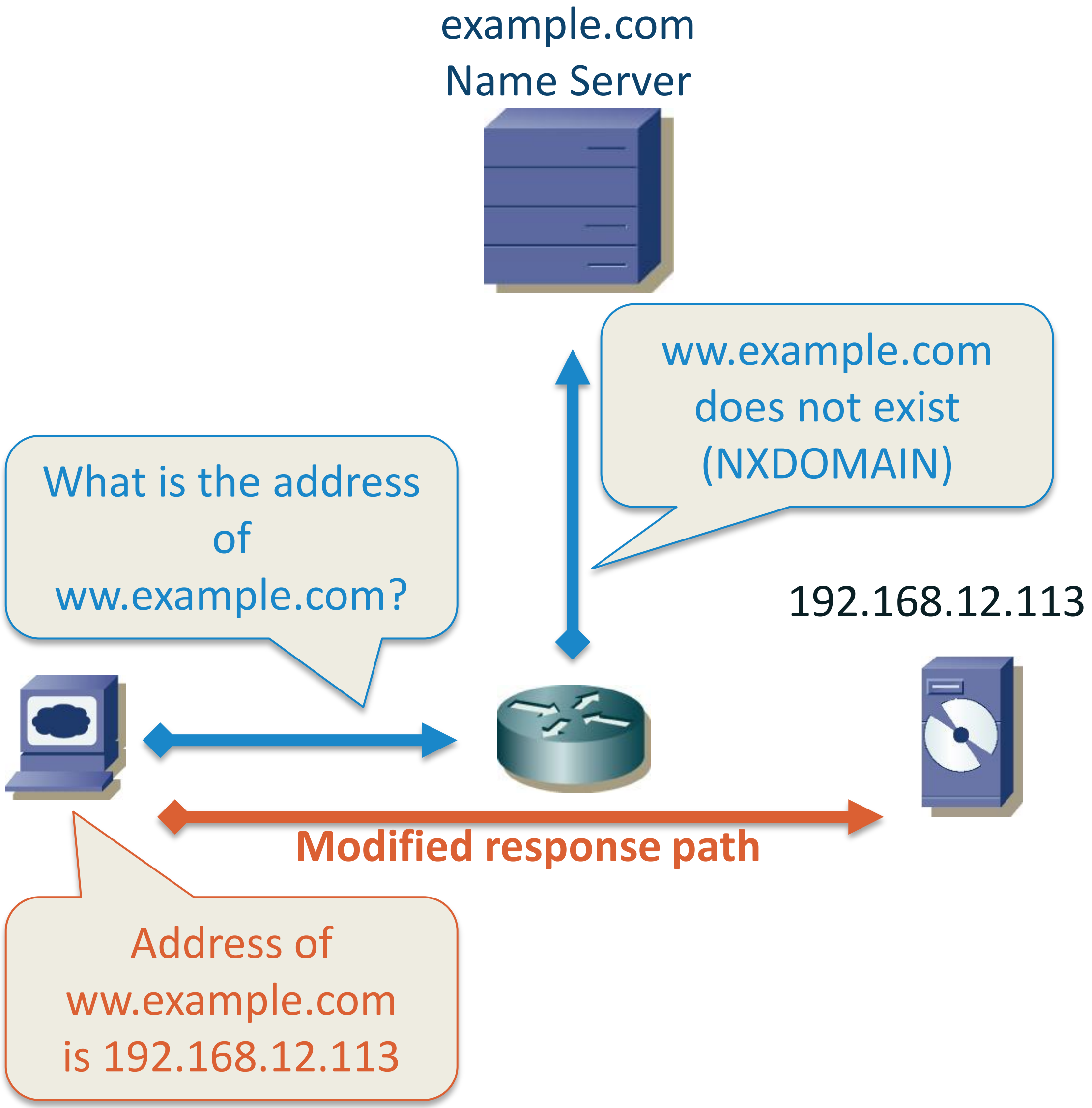
Redirected path

Redirected path

Bank Web Site

Intended path for online banking transactions

Response Modification



example.com
Name Server

www.example.com
does not exist
(NXDOMAIN)

What is the address
of
www.example.com?

192.168.12.113

Modified response path

Address of
www.example.com
is 192.168.12.113

- Recursive resolver is configured to return IP address of web, pay-per-click, or search page when it receives NXDOMAIN response
- Also used by ISPs and 3rd parties for monetizing purposes

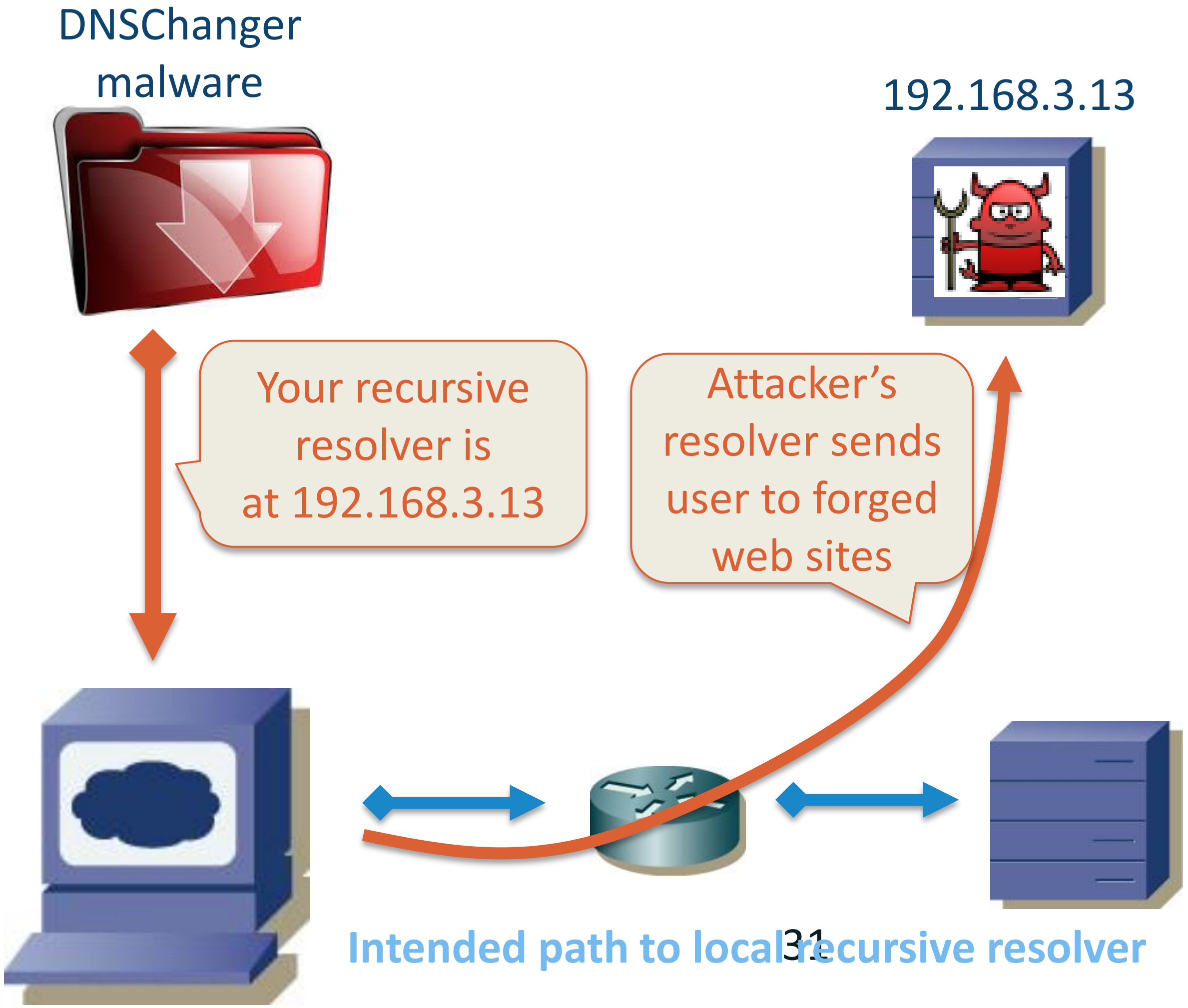
Configuration Poisoning: DNSChanger

Attacker distributes DNS configuration altering malware via

- Spam, drive-by download…

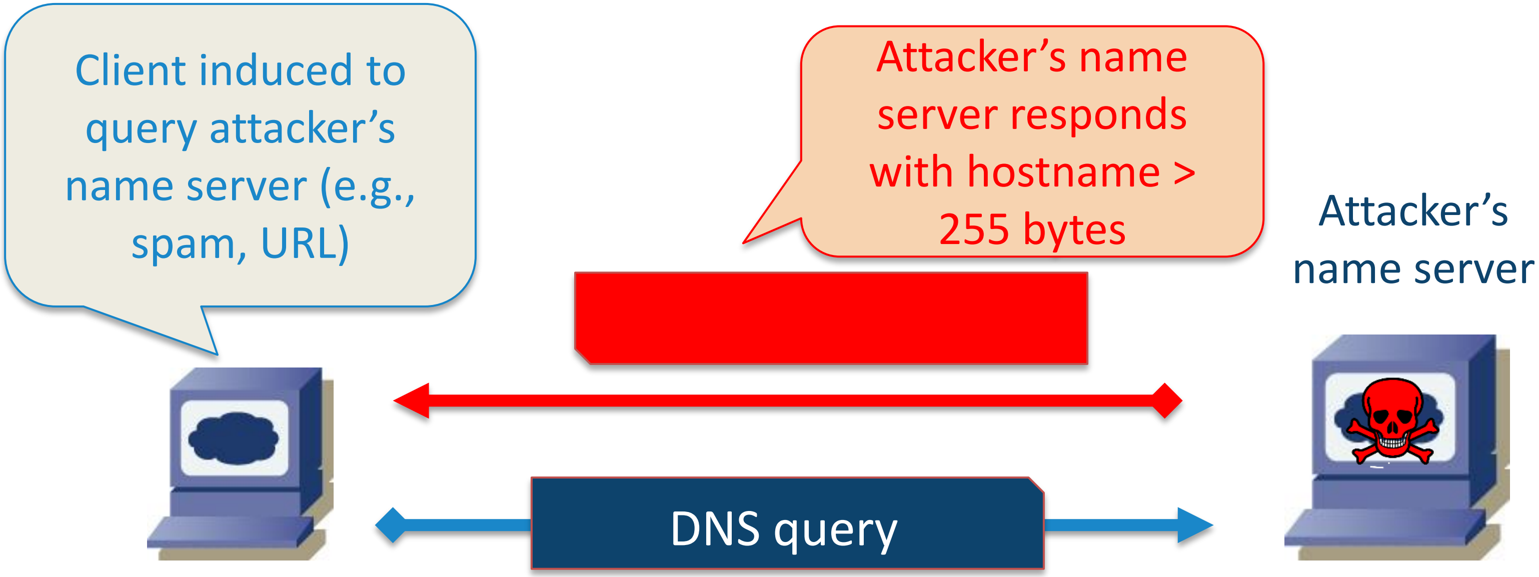
DNSChanger malware

- Alters DNS configuration of infected PC
- Causes all requests to go to a malicious name server run by attackers
- Attacker updates malware to redirect web traffic to a destination of his choosing


DNSChanger malware
192.168.3.13
Your recursive resolver is at 192.168.3.13
Attacker's resolver sends user to forged web sites
Intended path to local recursive resolver
31

DNS hostname overflow attack

- Attacker crafts response message containing domain name > 255 bytes
- *Vulnerable* client queries attacker's name server, fails to check hostname length in response
- Buffer overflow allows a attacker to gain root or execute arbitrary commands

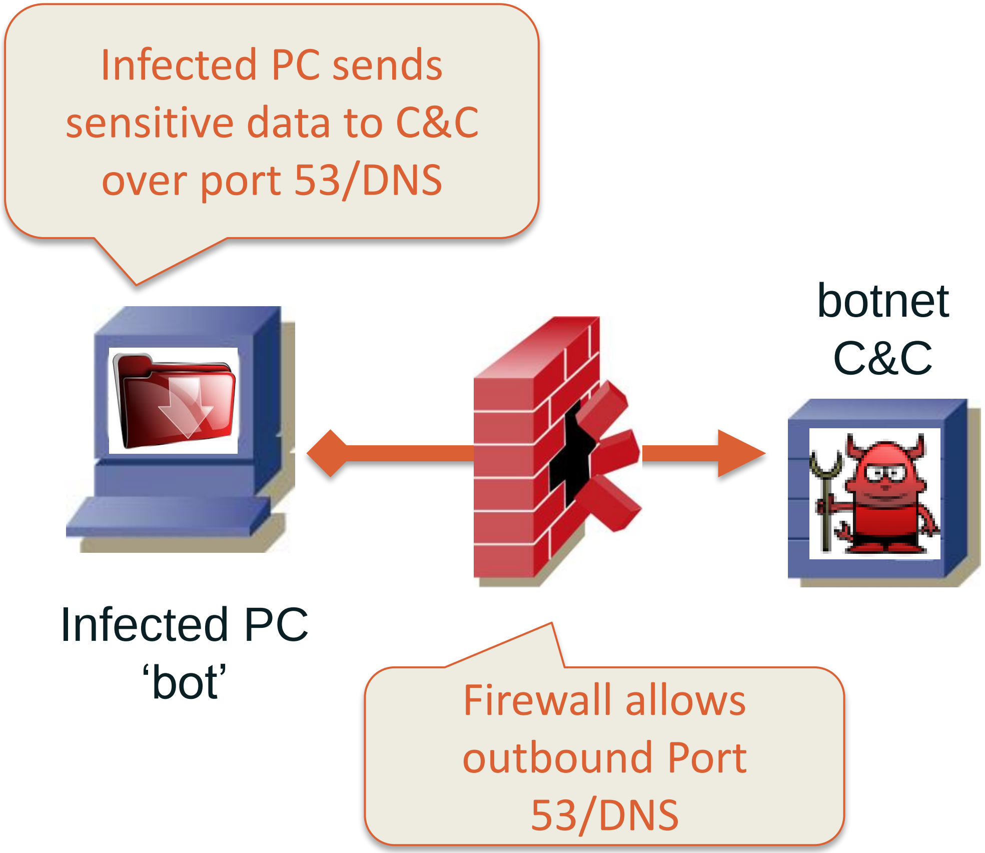

Client induced to query attacker's name server (e.g., spam, URL)
Attacker's name server responds with hostname > 255 bytes
Attacker's name server
DNS query

DNS and registration system misuse

- DNS as a Covert Exfiltration Channel
- DNS as a Covert Malware Channel
- Fast Flux
- Domain hijacking, DNS hijacking

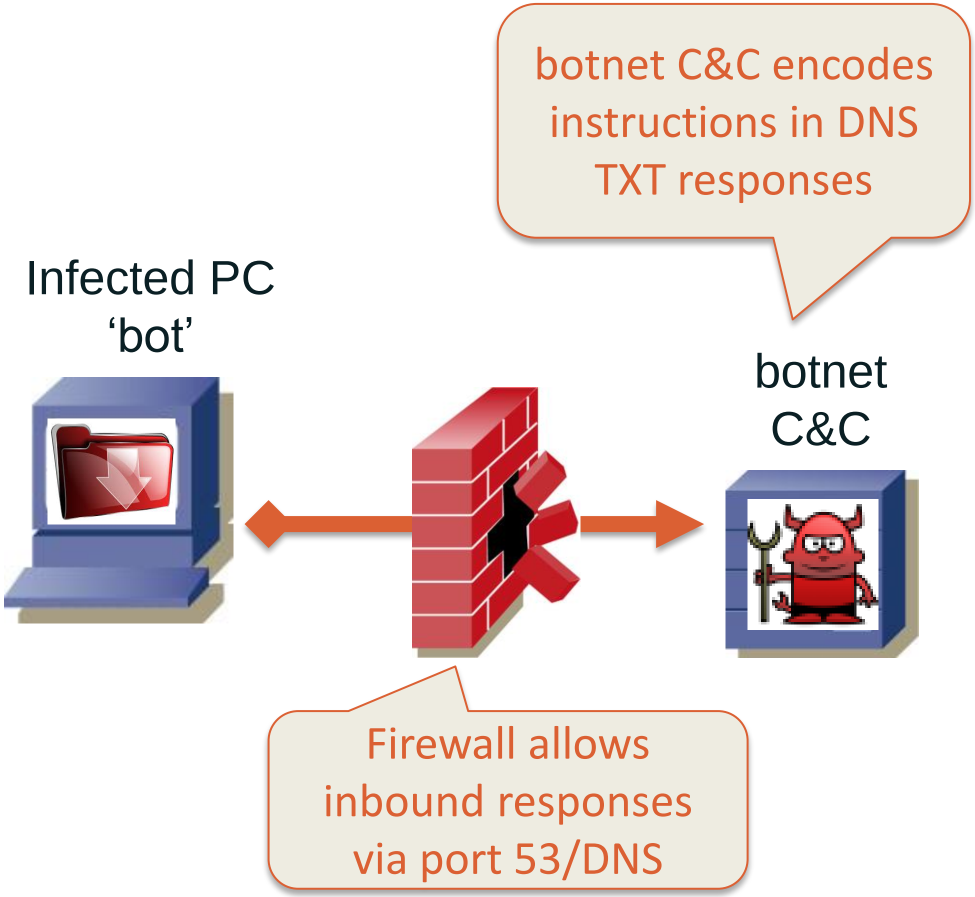
Let’s look at some examples

DNS as a Covert Exfiltration Channel


Infected PC sends sensitive data to C&C over port 53/DNS
botnet C&C
Infected PC 'bot'
Firewall allows outbound Port 53/DNS

- DNS messages manipulated to forward sensitive data from infected PC *through firewall* to botnet command and control (C&C)
- Proof of concept: exfiltrate results of SQL injection attacks

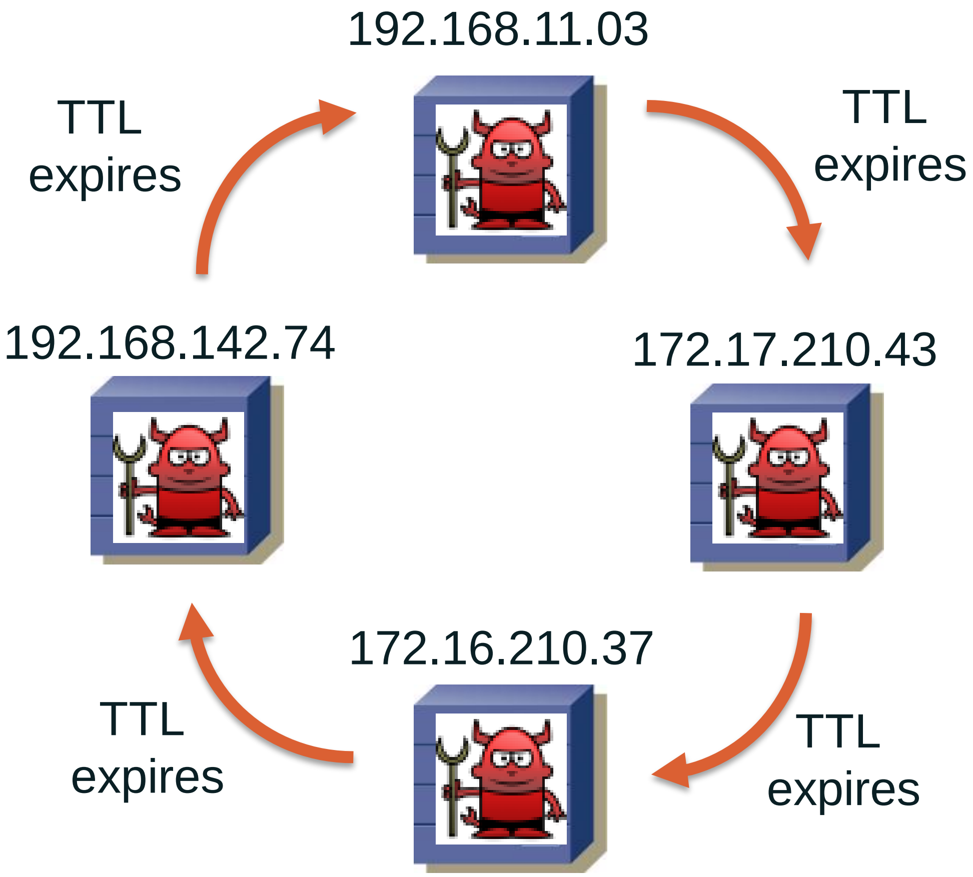
DNS as a Covert Malware Channel


botnet C&C encodes instructions in DNS TXT responses
Infected PC 'bot'
botnet C&C
Firewall allows inbound responses via port 53/DNS

- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions for bot
- Examples in wild:
  - Feederbot
  - Morto

Fast Flux Botnet

- Attacker
  - Associates IP address with a web host or DNS server for short time to live (TTL)
  - Changes IP of host or name server at low TTL frequency to thwart investigators



Domain registration hijacking

- Attacker compromises registration account, e.g.,
  - Succeeds with brute force, social engineering, or login attack
  - Launches a *registrar impersonation phishing attack*
  - Compromise gives attacker administrative control over domains registered under this account
- Attacker modifies/adds name server record for domain
  - NS record that is published in TLD zone associates domain's name server with IP address of attacker's host
- Attacker publishes "attack" zone data
  - Resource records in zone data support phishing, fraud, or defacement sites, spam mail exchanges, VoIP servers…

Note: An attacker can also compromise a name server directly

Summary

1 The DNS is an open system and *open also to abuse*

2 The DNS is a critical Internet database and thus a *target* for attack

3 Any element of the DNS may be *exploited* to facilitate other attacks

Agenda

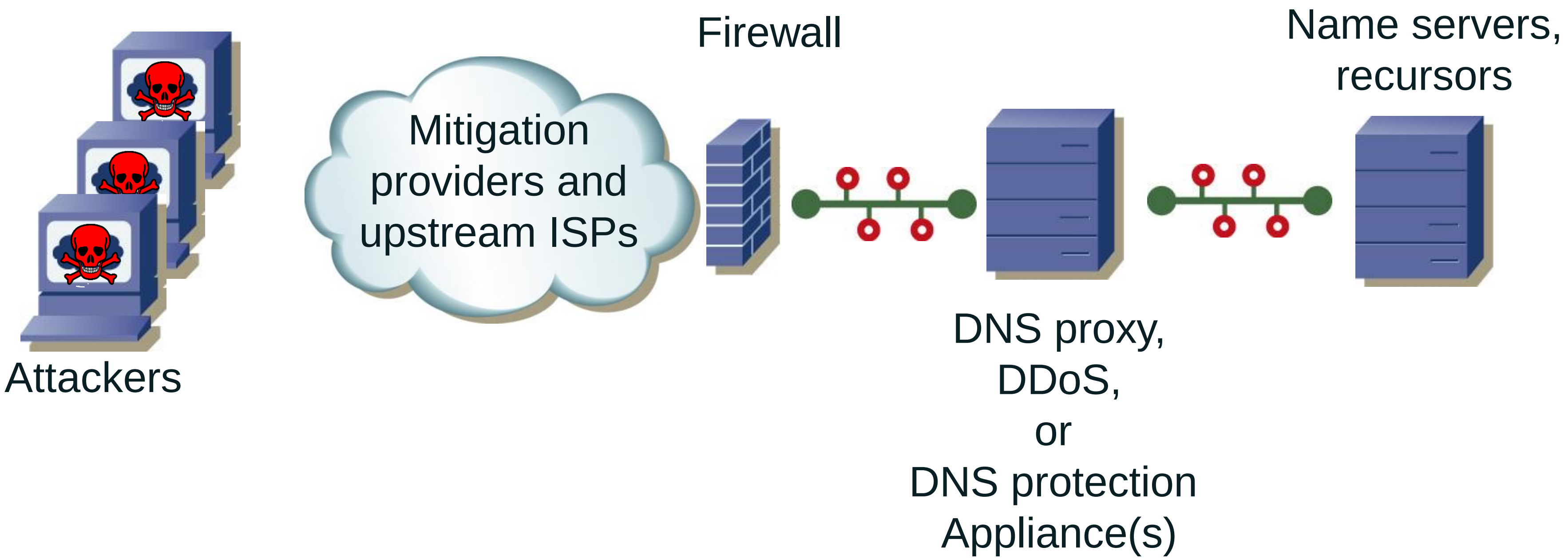
- How does the DNS work?
- Attacking the DNS
- Attack mitigations and countermeasures

People and Resource planning

- Identify
  - Vulnerabilities
  - Bottlenecks
  - Capacities
- Plan
  - Initial Response and Abatement
  - Escalation
  - Upstream allies
- Intelligence
  - Information to help you identify whether you are a potential target, and why

DNS Defense in Depth

- Interpose layers of defense between attacker and DNS infrastructure
- Add diversity and redundancy to infrastructure


Firewall
Name servers, recursors
Mitigation providers and upstream ISPs
Attackers
DNS proxy, DDoS, or DNS protection Appliance(s)

Best Practices ("Best" if universally employed)

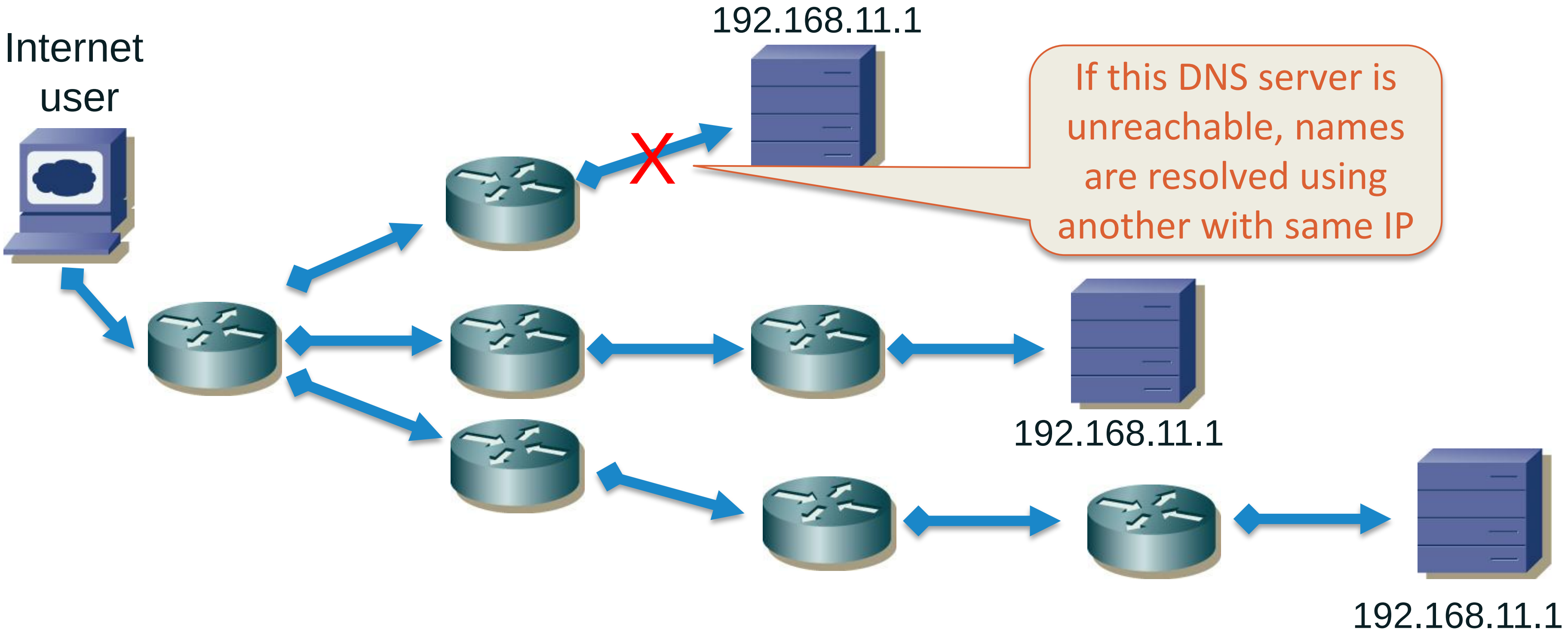
- Eliminate IP-spoofing (BCP 38)
  - Ingress Source Address filtering
  - Remotely Triggered Black Holing (RTBH)
  - Unicast Reverse Path Forwarding (uRPF)
  - ASN or Prefix Blocklisting
- Eliminate open resolvers (BCP 140)
  - Configure resolvers to only respond to queries from authorized users or applications
  - Enable logging and (threshold) monitor

Recommended DoS Mitigation measures

- Anycast routing
- DNS service segregation
- DNS intrusion defenses
- Redundancy and diversity measures
- TCP Flood abatement measures
  - SYN Proxies, SYN Cache, or SYN Cookies
- Over-provisioning

Anycast routing for resolvers or authoritatives

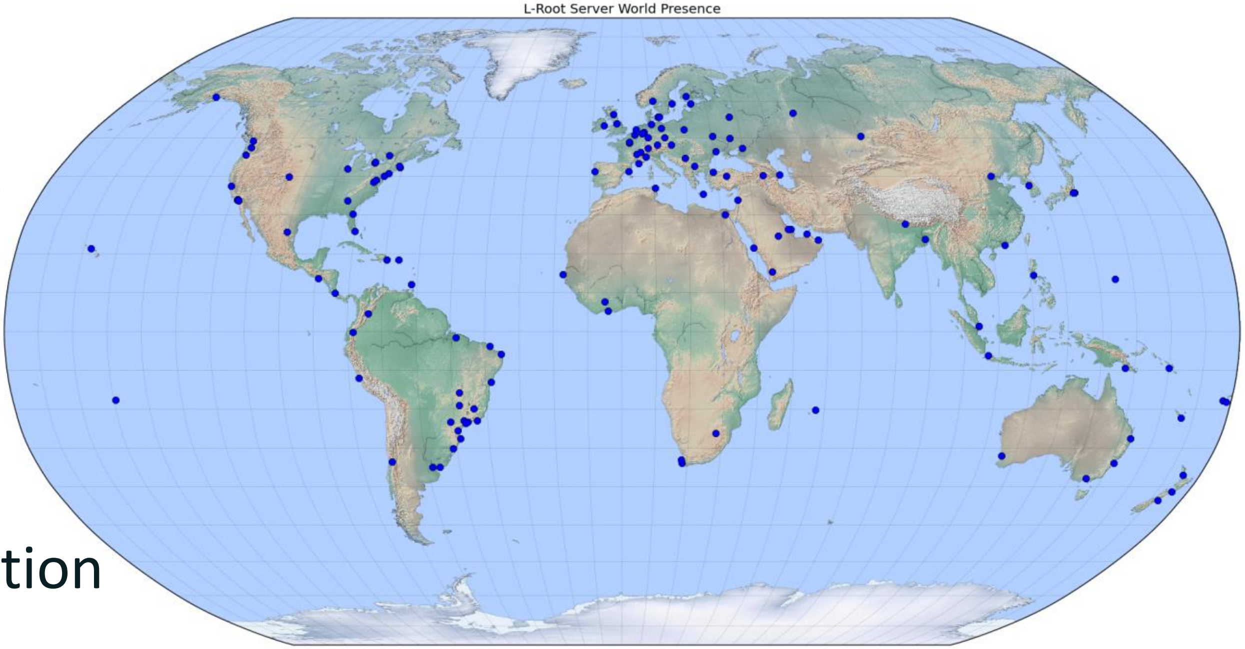
- Unicast: one DNS host, one IP address
- Anycast: many DNS hosts, one IP address
  - Routing forwards to closest available



If this DNS server is unreachable, names are resolved using another with same IP

Example: Root Name System and Anycast DNS

- Diversity:
  - Geography
  - Hardware
  - Software
  - Bandwidth
  - Administration
- Redundancy
  - Failover
  - Load balancing



DNS Service Segregation

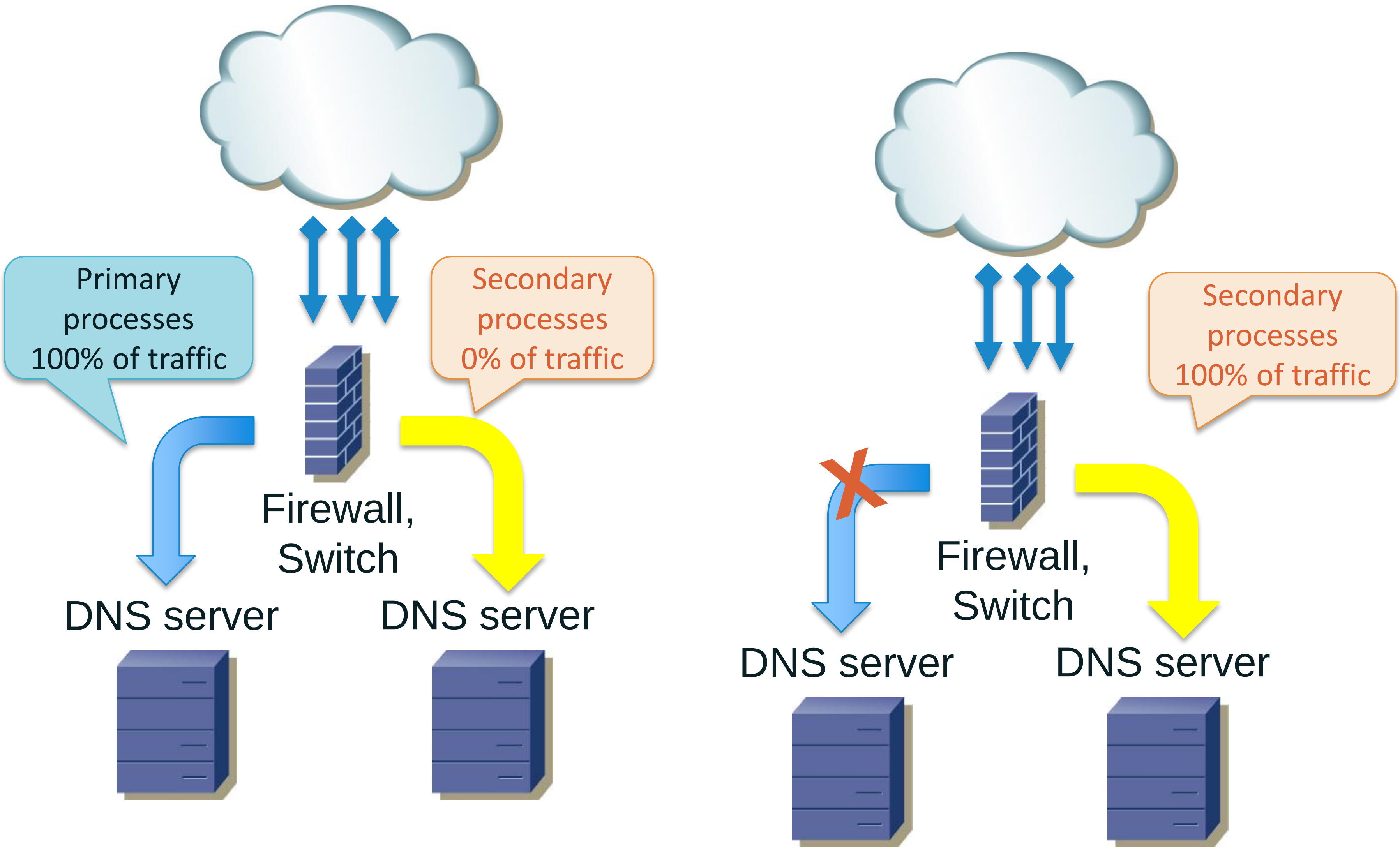
- Design network topology so that critical infrastructure is protected against side attacks
- Run DNS services on separate network segments from other services
- Run authoritatives on separate network segments from recursors
- Separate client networks from services
- Customized defenses for each segment

DNS Intrusion Defenses

DNS intrusion defenses are implemented on premises at switches, routers, firewalls, security appliances or by mitigation providers

DNS Access Controls	DNS Volumetric Attack Detection
Spoofed source addresses	Excessive Name errors
Malformed or suspicious queries	
Malformed or suspicious responses	Atypical DNS message sizes
Message length anomalies	
Known bad/suspicious traffic origins	Atypical use of TCP
Known bad/suspicious domains	
Known malicious/covert traffic patterns	Deviations from historical or planned traffic volume
Network traffic anomaly protection	
Source or connection response rate limiting	

DNS Redundancy (Failover)

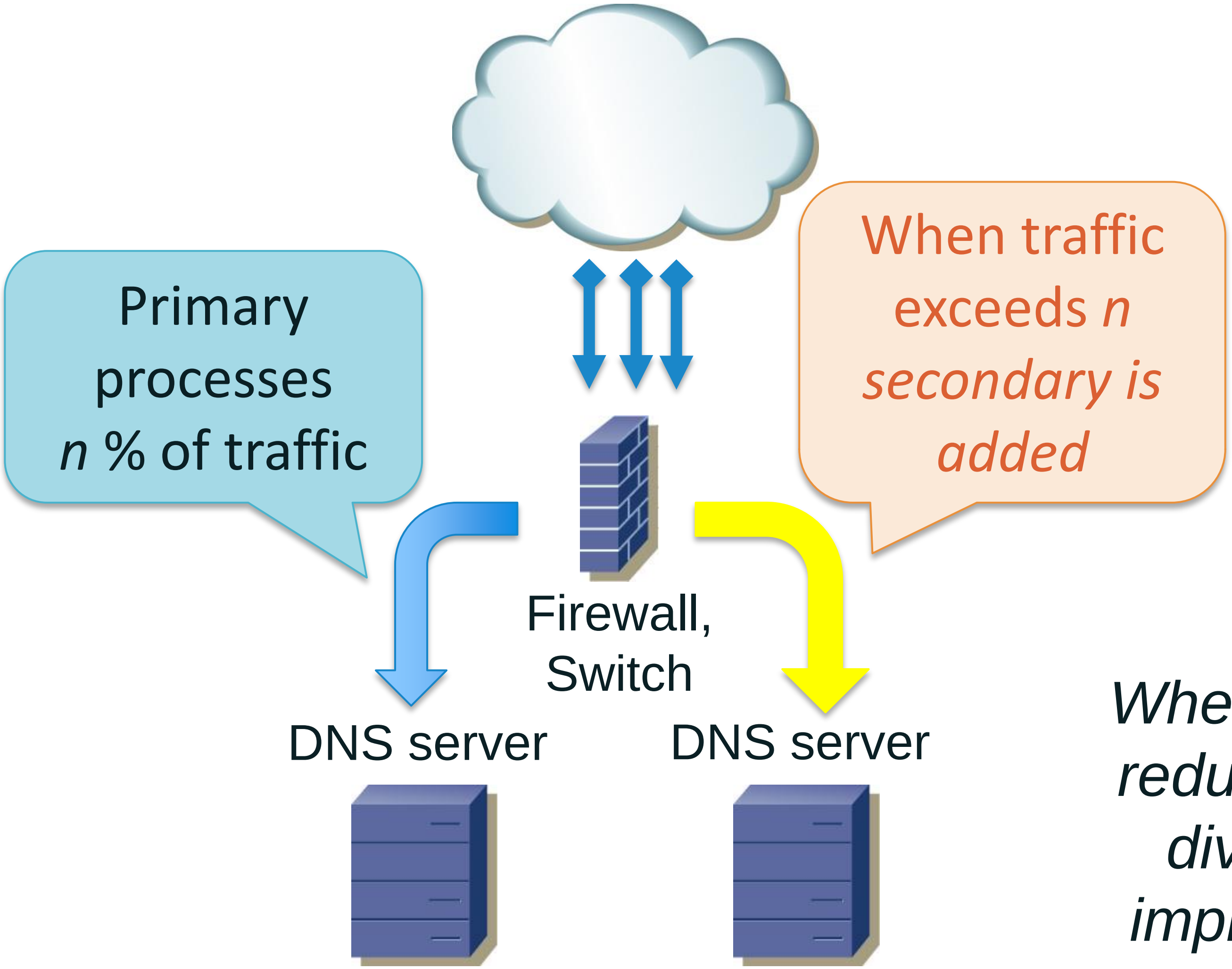


Primary processes 100% of traffic

Secondary processes 0% of traffic

Secondary processes 100% of traffic

Redundancy (Load Balancing)



Primary processes *n* % of traffic

When traffic exceeds *n* *secondary is added*

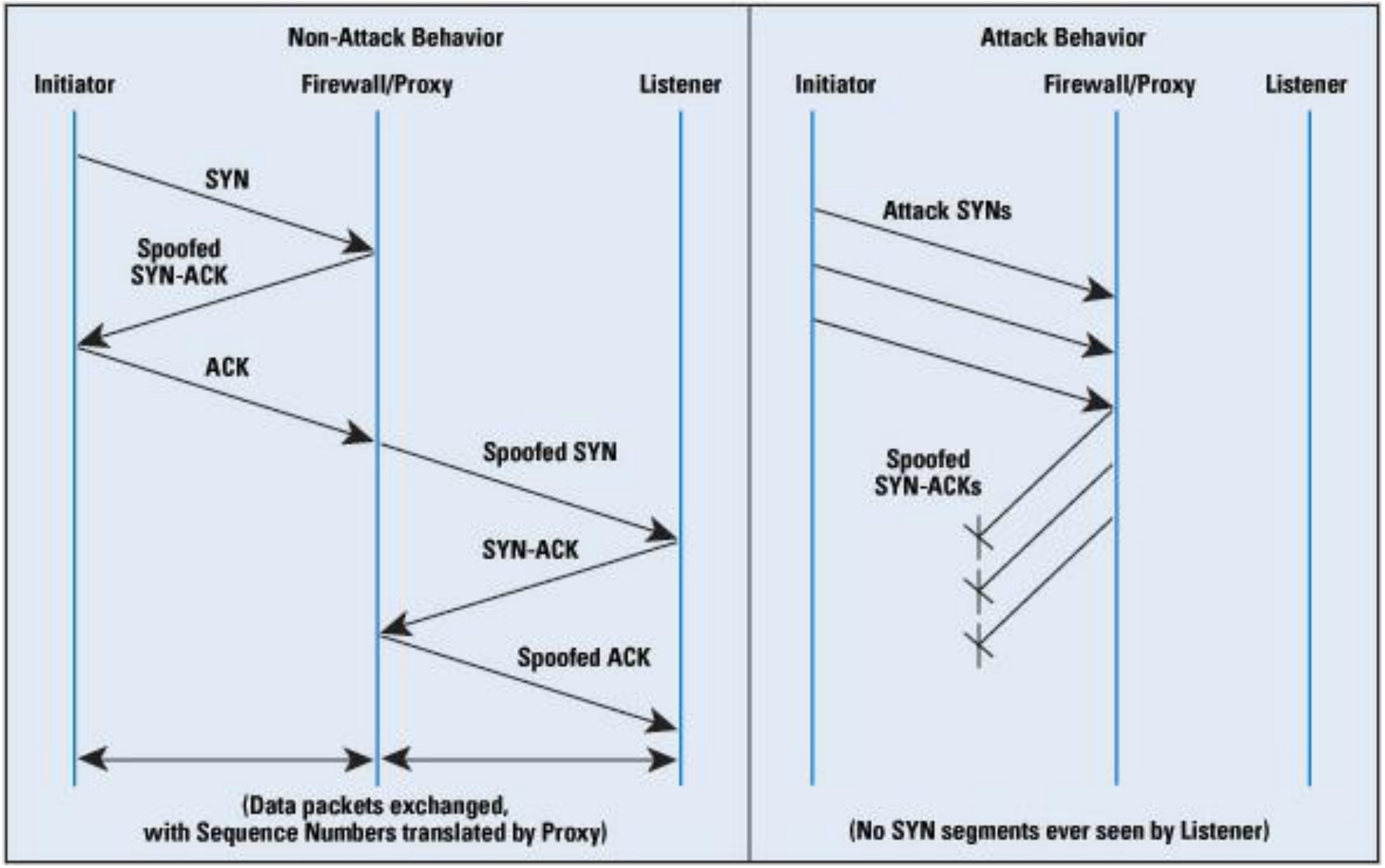
Firewall, Switch

DNS server

DNS server

Where else can redundancy or diversity be implemented?

TCP abatement strategies



Over-provisioning

https://www.flickr.com/photos/59937401@N07/

Deploy more capacity than

- you can conceivably consume
- attackers can overwhelm using volumetric attacks
- a.k.a. “Mother’s Day” capacity planning

Homework: look up Neal-Wilkinson and Erlang B Peaked Traffic models

Configuration Management

- Keep software or firmware up to date
  - Operating systems
  - Name server software
  - Security and network systems
- Validate and archive
  - “last known working” configurations
  - zone data
  - Infrastructure topology

Real time policy enforcement

- Enforce DNS behavior and traffic policies
- Detect or drop – and log
  - DNS malformed traffic
  - “Known malicious” or suspicious DNS traffic patterns
  - Name error responses

Image by dingcarrie

Real time event monitoring

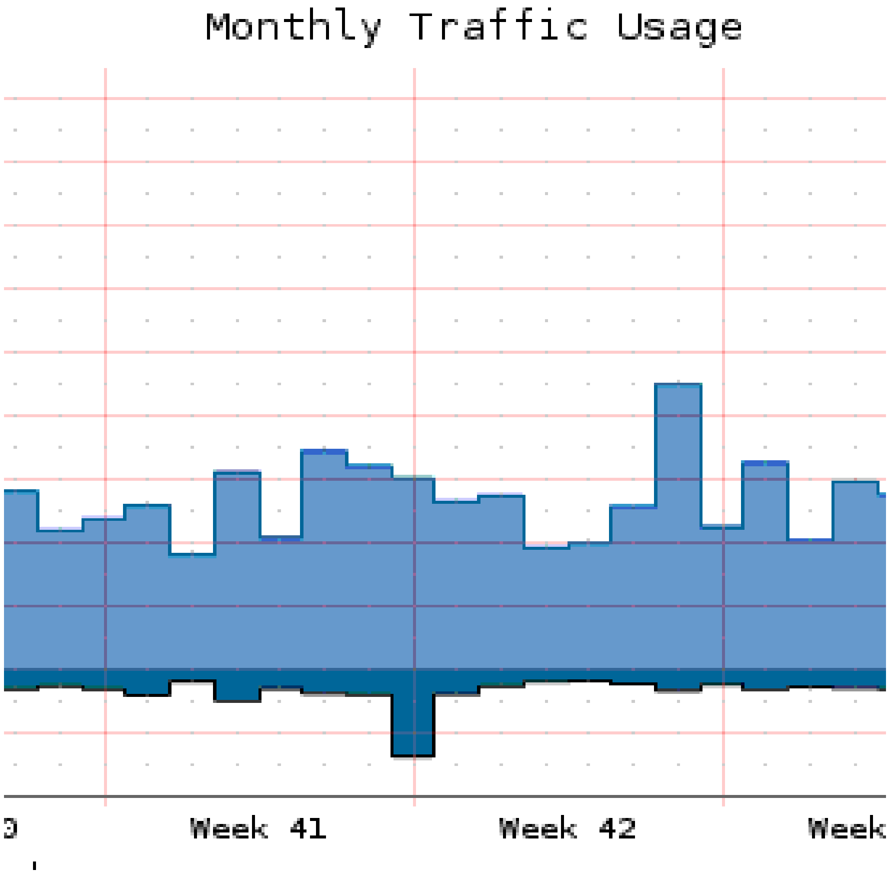


Image by Jo mangee

- At name servers and recursors
  - DNS process and traffic logging
  - Operating system process and event logging
  - Threshold-based alerts

Periodic Analysis

- Examine critical data for “correctness”
  - DNS zone data
  - Recursor caches
- Passive DNS replication
  - Review what names your users are resolving
  - Review name errors

Resource and Relationship Management

- Points of contact for
  - Mitigation providers
  - Upstream ISPs
  - Hosting providers
  - Vendors and security service technical support
  - CERTs
  - Friendlies, e.g., security community
  - Law enforcement
  - Regulatory authorities (if applicable)

Domain name registration protection

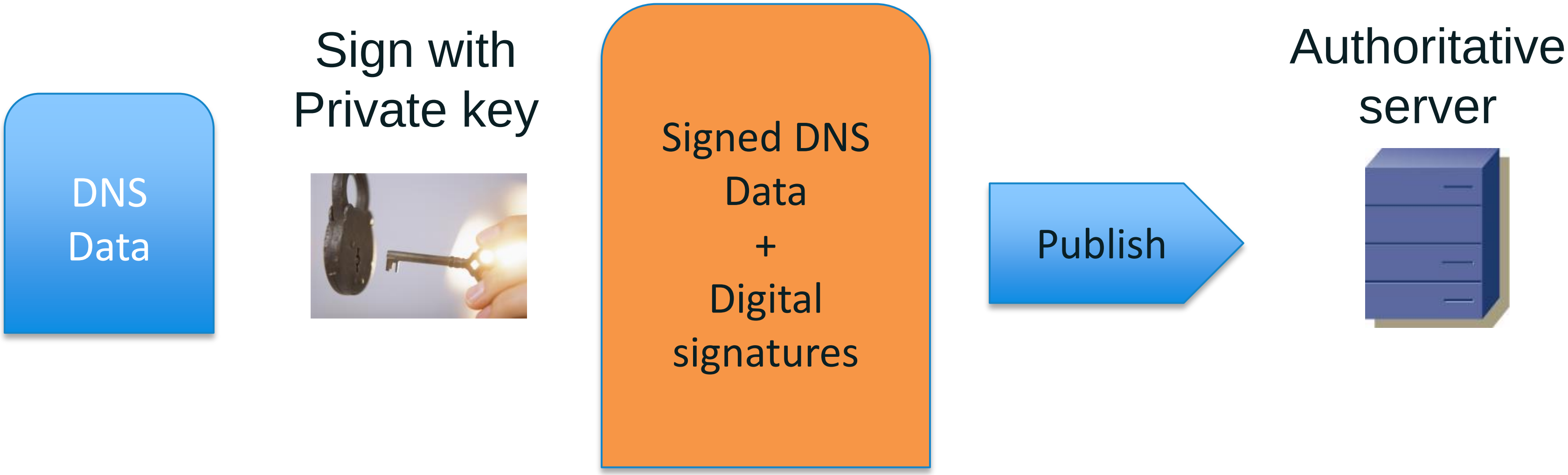
- Maintain complete/accurate points of contact
- Monitor Whois record for unauthorized change
- In case of unauthorized transfer, keep records
  - Domain names, proofs of payments, registrar correspondence
  - Demonstrations of use: system/web logs, site archives
  - Legal documents: proofs of incorporation, tax filings, passport, other proofs of identity
  - Any documentation that demonstrates an association between the domain name and *you*

DNS Security (DNSSEC)

- Protects DNS data against forgery
- Uses public key cryptography to sign authoritative zone data
  - Assures that the data origin is authentic
  - Assures that the data are what the authenticated data originator published
- Trust model also uses public key cryptography
  - Parent zones sign public keys of child zone (root signs TLDs, TLDs sign registered domains…)

Public Key Cryptography in DNSSEC

- Authority signs DNS data with *private* key
  - Authorities must keep private keys secret!
- Authority publishes *public* key for everyone to use



DNS Data

Sign with Private key

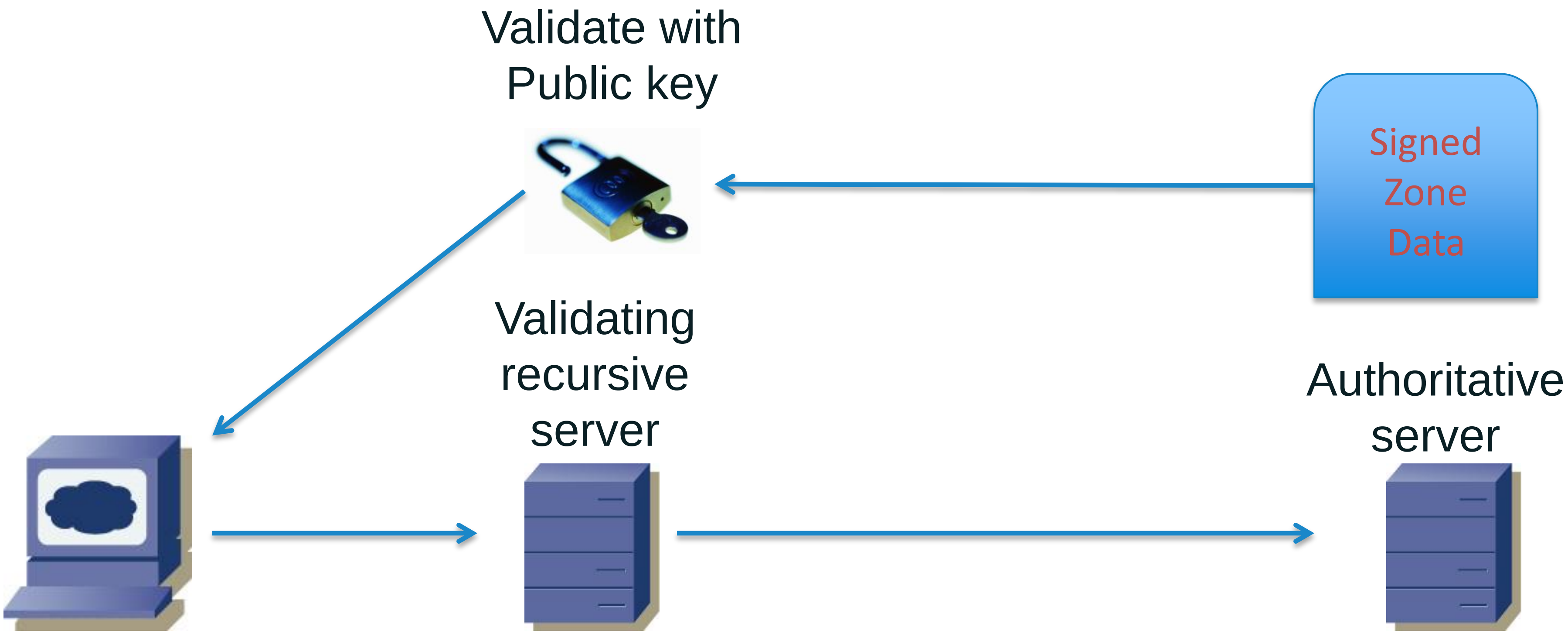
Signed DNS Data + Digital signatures

Publish

Authoritative server

Public Key Cryptography in DNSSEC

- Any recipient of the authority’s DNS data can use the public key to verify that “the data are correct and came from the right place”



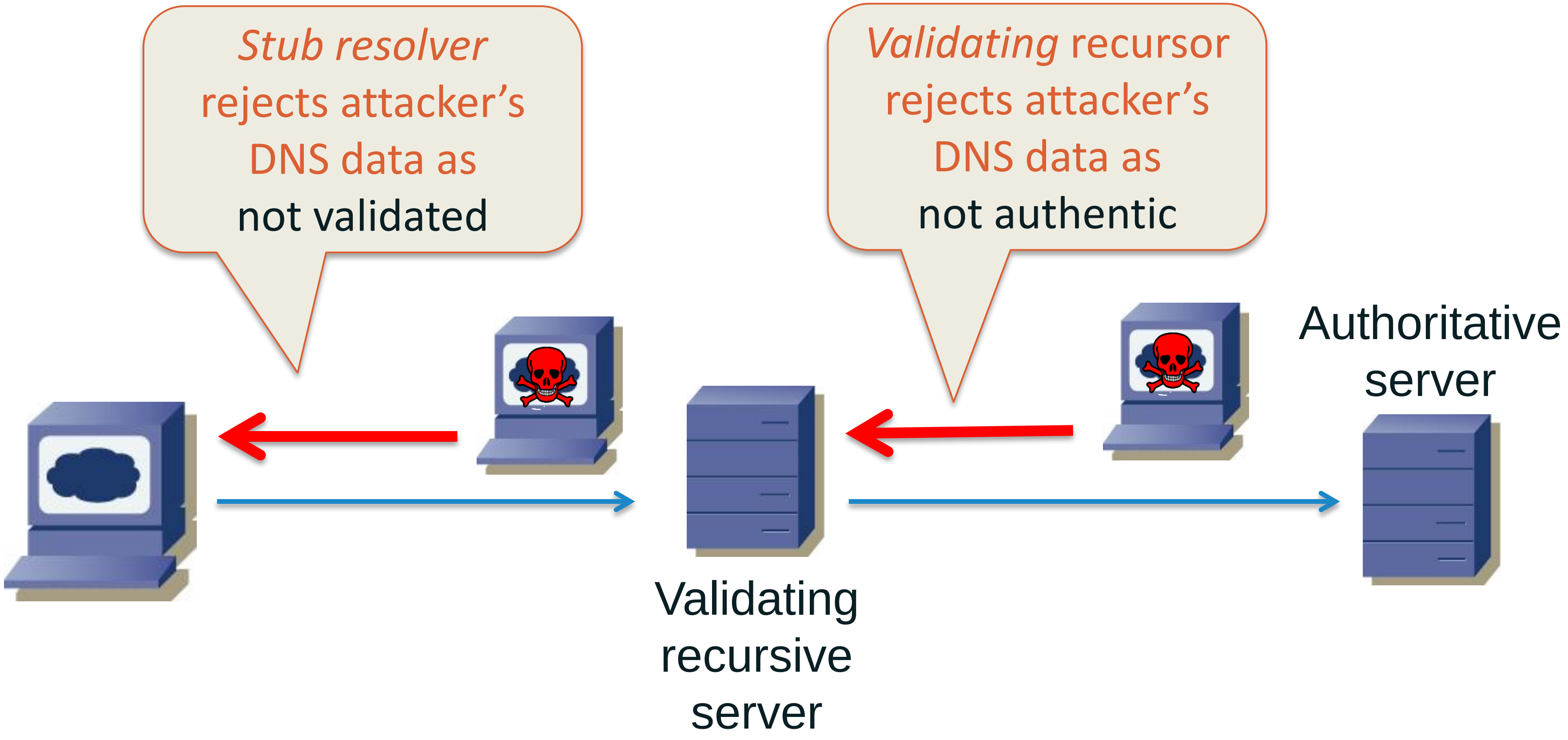
Validate with Public key

Signed Zone Data

Validating recursive server

Authoritative server

How DNSSEC defeats data poisoning attacks



Stub resolver rejects attacker's DNS data as not validated

Validating recursor rejects attacker's DNS data as not authentic

Authoritative server

Validating recursive server

Summary

1 Implement an in-depth defense to mitigate DNS attacks

2 Some mitigations require allies or broad implementation

3 Some of the best mitigations are "soft" (planning or administrative)

Reading list (Partial)

Title	URL
Top 10 DNS attacks	http://www.networkworld.com/article/2886283/security0/top-10-dns-attacks-likely-to-infiltrate-your-network.html
Manage your domain portfolio	http://securityskeptic.typepad.com/the-security-skeptic/2014/01/avoid-risks-manage-your-domain-portfolio.html
Securing open DNS resolvers	http://www.gtri.com/securing-open-dns-resolvers-against-denial-of-service-attacks/
DNS Tunneling	https://www.cloudmark.com/releases/docs/whitepapers/dns-tunneling-v01.pdf
DNS cache busting	http://blog.cloudmark.com/2014/10/07/a-dns-cache-busting-technique-for-ddos-style-attacks-against-authoritative-name-servers/
DNS Cache Poisoning	http://www.securityskeptic.com/dns-cache-poisoning.html
Anatomy of a DDOS attack	http://www.securityskeptic.com/anatomy-of-dns-ddos-attack.html
DNS reflection defense	https://blogs.akamai.com/2013/06/dns-reflection-defense.html
Protect the world from your network	http://securityskeptic.typepad.com/the-security-skeptic/2013/04/protecting-the-world-from-your-network.html
DNS Traffic Monitoring Series	http://www.securityskeptic.com/2014/09/dns-traffic-monitoring-series-at-dark-reading.html
Protect your DNS servers against DDoS attacks	http://www.gtcomm.net/blog/protecting-your-dns-server-against-ddos-attacks/
Fast Flux Botnet Detection in Realtime	http://www.iis.sinica.edu.tw/~swc/pub/fast_flux_bot_detection.html
DNS resource exhaustion	https://www.cloudmark.com/releases/docs/whitepapers/dns-resource-exhaustion-v01.pdf

Questions?

My Contact Info:

- dave.piscitello@icann.org
- @securityskeptic
- www.securityskeptic.com
- about.me/davepiscitello

Contact ICANN:

- engagement@icann.org
- @icann
- icann.org
- safe.mn/icannsecurityteam