Attacks Against The DNS, DNS Monitoring & Countermeasures

Dave Piscitello
VP Security and ICT Coordination
27 June 2016
dave.piscitello@icann.org

Introduction

- VP Security and ICT Coordination, ICANN
- 40 year network and security practitioner
- Roles at ICANN:
  - Technology Advisor
  - Threat responder
  - Investigator
  - Researcher

Agenda

- Overview of the DNS attack landscape
- Attack mitigations and countermeasures
- DNS Monitoring

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 attack
- Resource Depletion (Exhaustion) attacks

Attacks Involving Stub Resolvers

- Query interception attack
- DNS Response modification
- Configuration poisoning attack
- DNS hostname overflow attack
- DNS as a Covert Exfiltration Channel
- DNS as a Covert Malware Channel

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

- Overview of the DNS attack landscape
- Attack mitigations and countermeasures
- DNS Monitoring

Begin With Resource And People Planning

- Inventory assets
- Assess and mitigate risks
  - Identify threats, vulnerabilities and bottlenecks
- Plan
  - Initial Response and Abatement
  - Escalation
- Conduct ongoing intelligence
  - Information to help you identify whether you or your industry are potential target, and why

Resource And Relationship Management

- Know your allies: Maintain 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)

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

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*

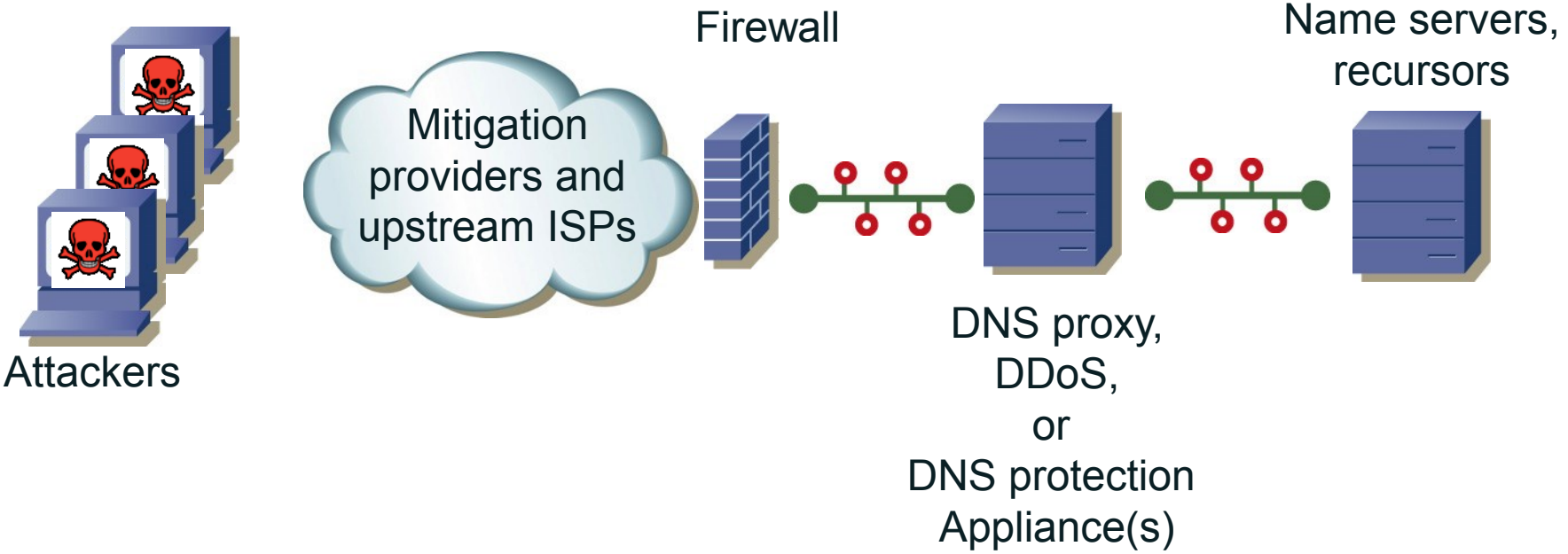
Be A Good Citizen

Don't let criminals use your resources to attack others

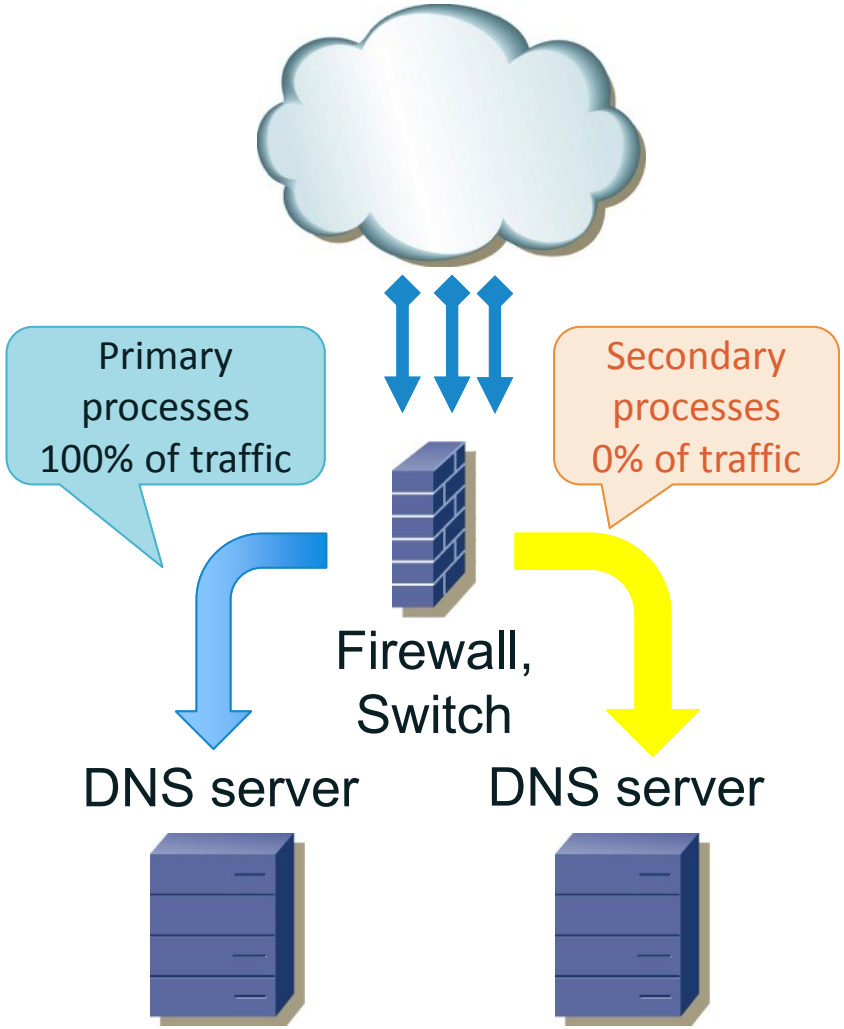
- Eliminate IP-spoofing (BCP 38)
  - Only allow traffic to exit your networks that uses addresses from blocks you use
- Eliminate open resolvers (BCP 140)
  - Configure your resolvers to only process DNS queries from your networks and hosts
- Add Response Policy Zones to your resolver
  - RPZs are lists of domain names that your name servers should not resolve

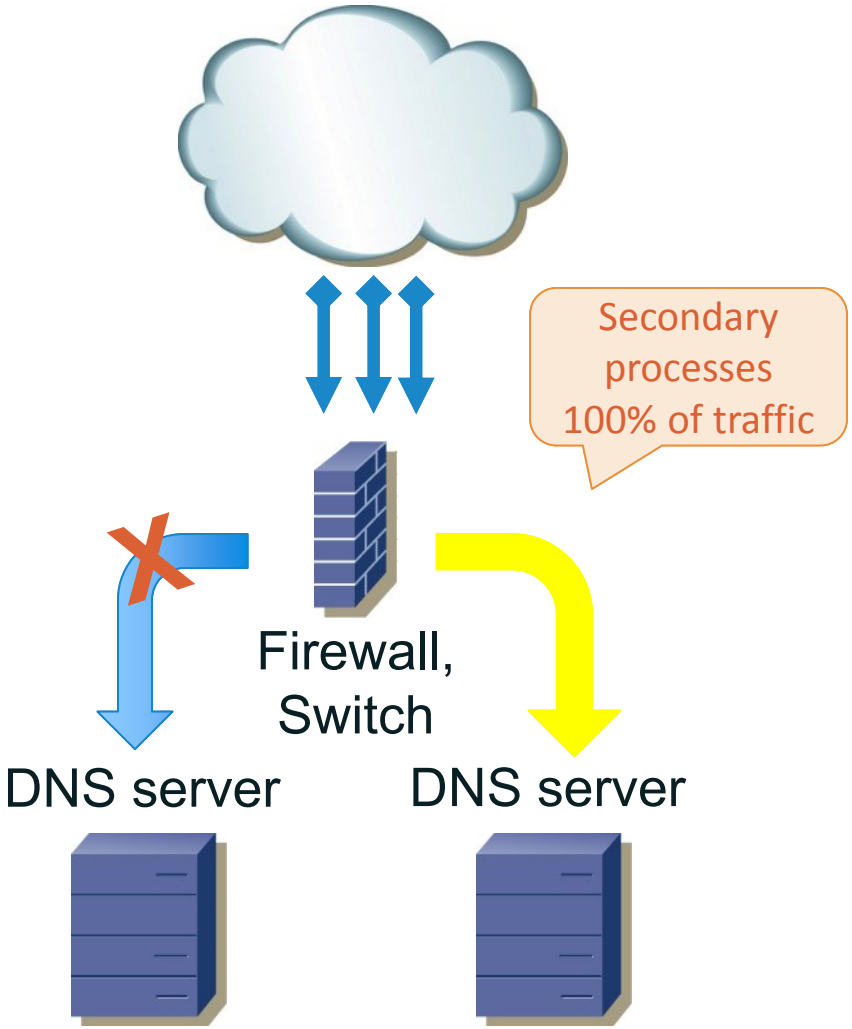
Deploy DNS Defenses in Depth

Interpose layers of defense between attackers and your DNS infrastructure

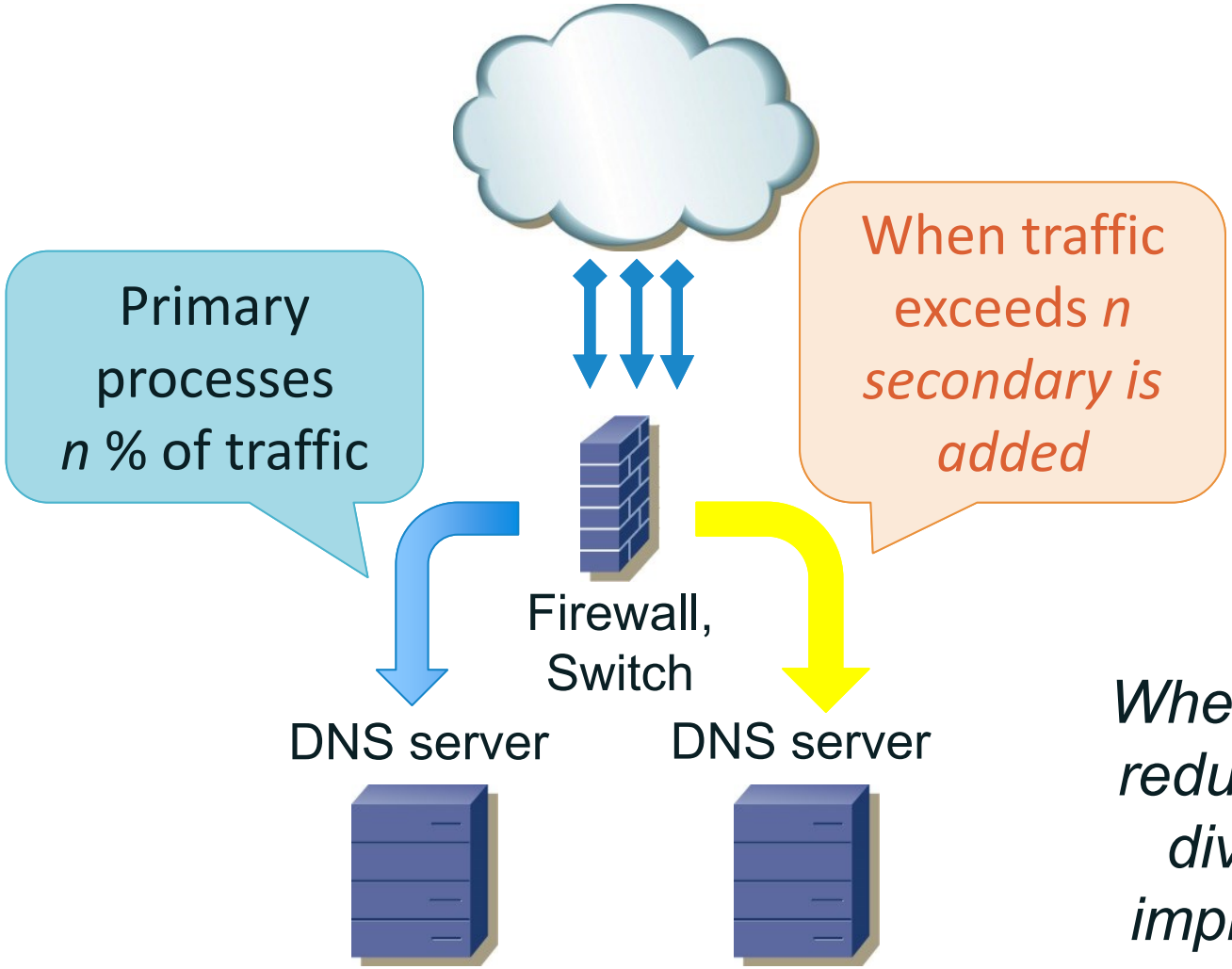


Add Redundancy To Your DNS: Fail Over





Add Redundancy To Your DNS: Load Balancing



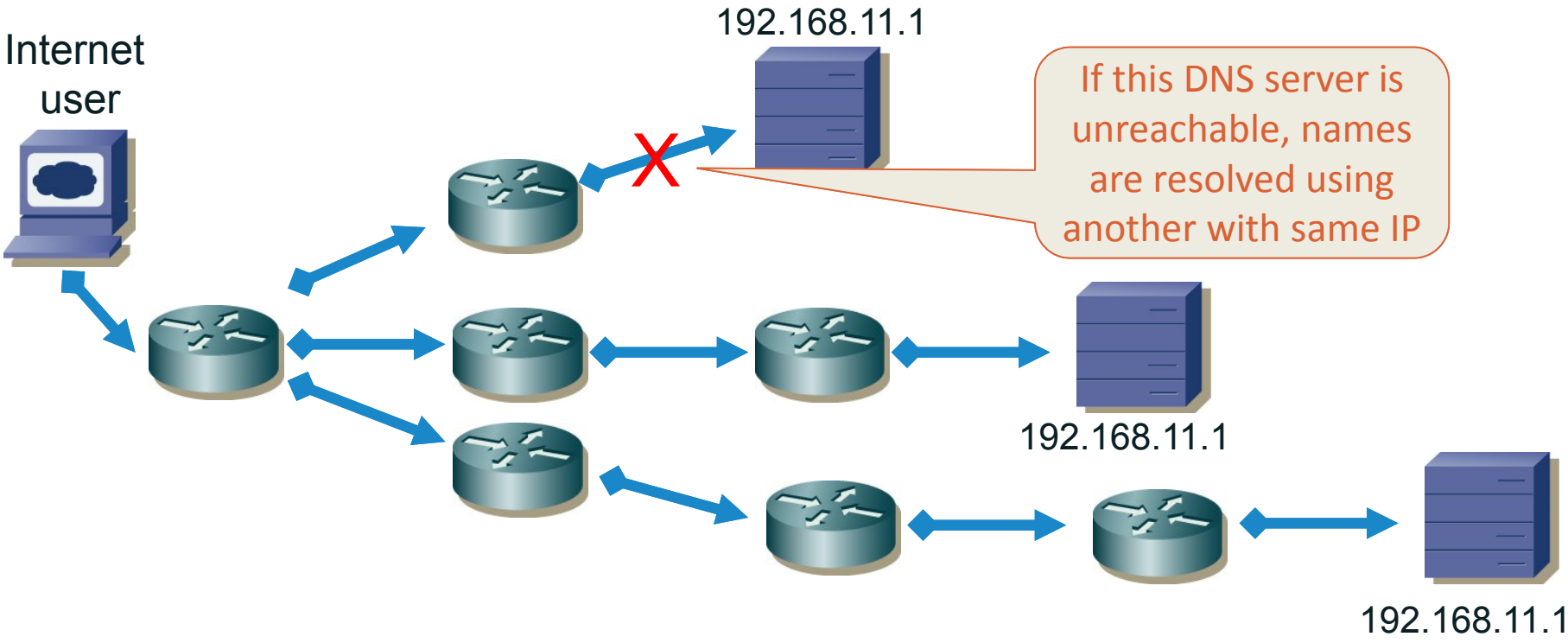
Where else can redundancy or diversity be implemented?

Recommended DoS Mitigation Measures

- Anycast routing
- DNS service segregation
- DNS intrusion defenses
- Redundancy and diversity measures
- Over-provisioning?

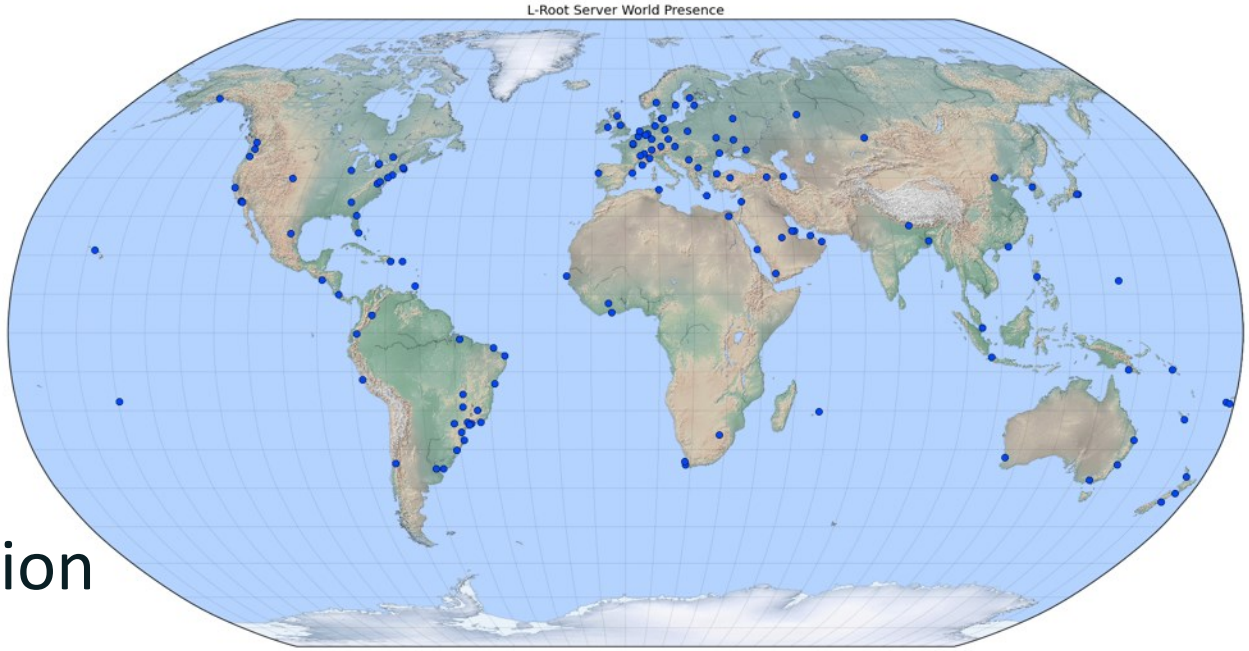
Anycast Routing For Name Servers

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



Example: Root Name System

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



DNS Service Segregation

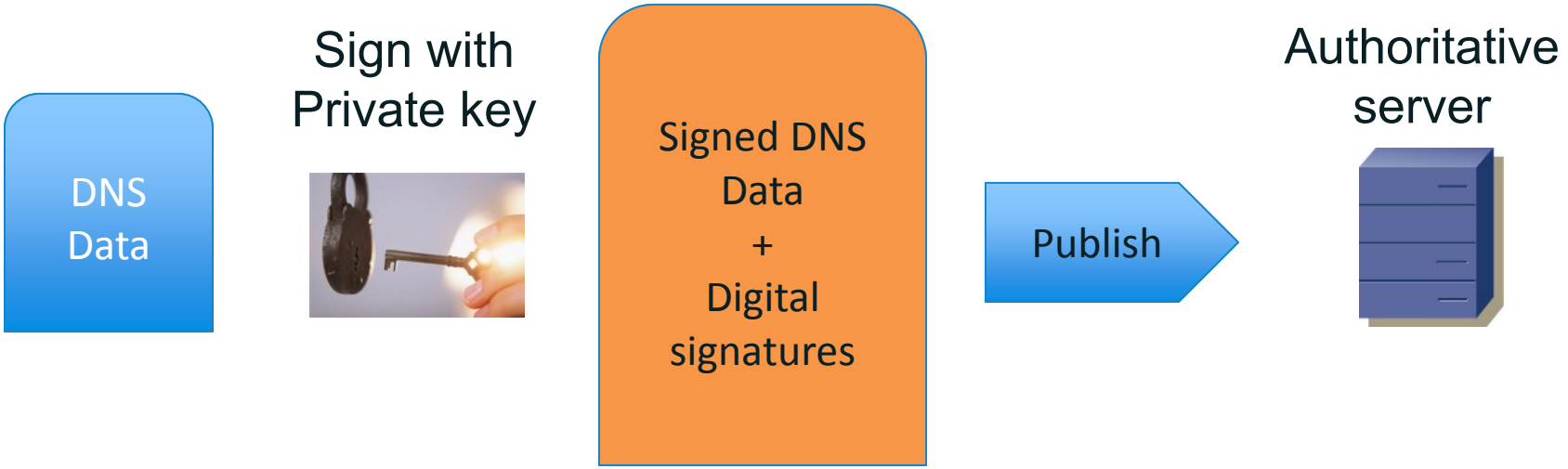
- Design network topology so that critical infrastructure is protected against side attacks
- Run DNS services on separate network segments from other services
- Run authoritatives on separate network segments from recursors
- Separate client networks from services
- Customized defenses for each segment

DNS 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…)

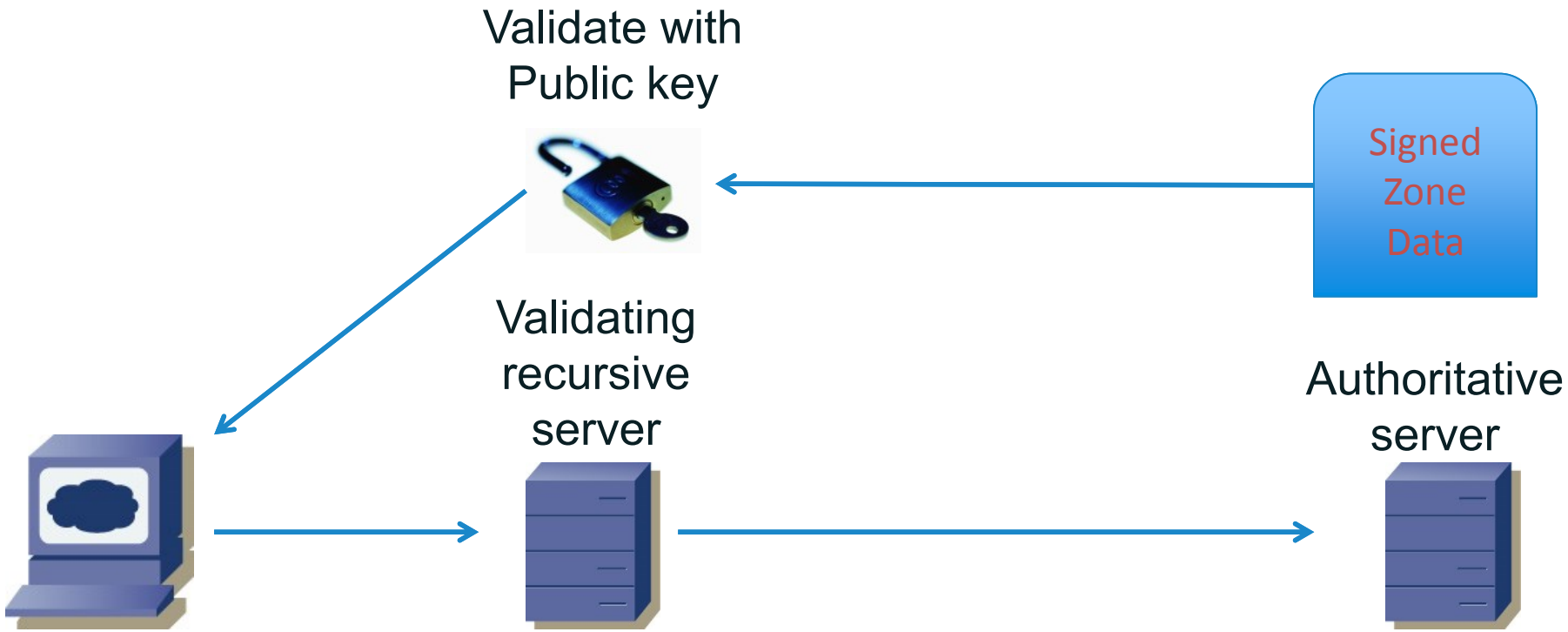
Public Key Cryptography in DNSSEC

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

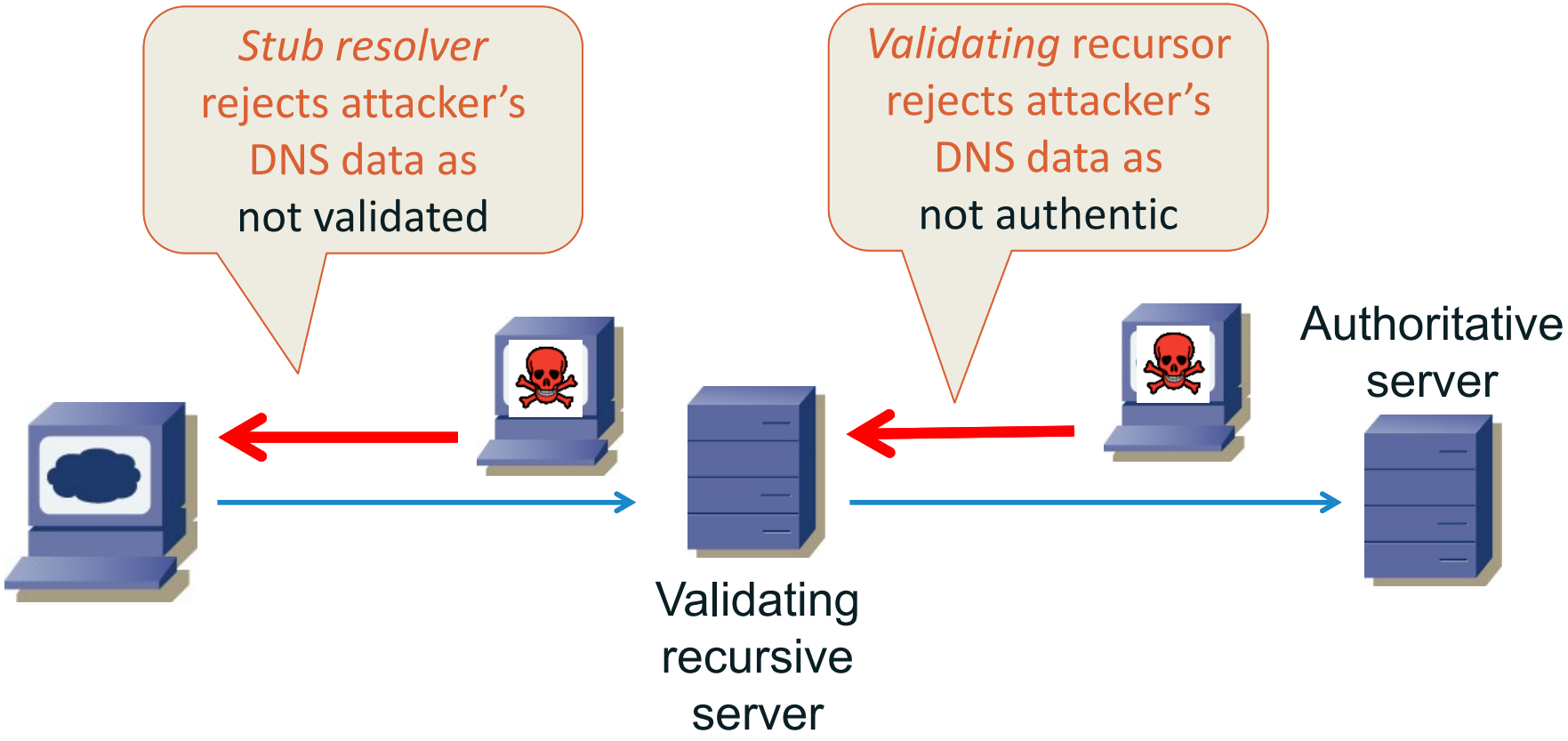


Public Key Cryptography in DNSSEC

- 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"



How DNSSEC defeats data poisoning attacks



Agenda

- Overview of the DNS attack landscape
- Attack mitigations and countermeasures
- DNS Monitoring

Real Time Traffic Analysis & Policy Enforcement

- Certain attacks change host configurations or resolver data
  - DNSchanger malware
  - Cache poisoners
- Track others by examining DNS traffic
- Enforce DNS behavior using access controls or intrusion detection
- Detect or drop – and log
  - DNS malformed traffic
  - “Known malicious” or suspicious DNS traffic patterns
  - Name error responses

Image by dingcarrie

Where to Look

- Host (device) or resolver configuration
- DNS query and response traffic on networks
- Resolver and authority logs
- Event logs
  - Hosts, Security Systems, Network elements
  - Applications (clients or servers)
- Passive DNS replication (sensor networks)

What To Look For

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	

How to Look

- Use traffic analyzers, Intrusion Detection Systems, or Internet firewalls to
  - Detect spoofing
  - Enforce egress traffic policy
  - Detect attempts to query unauthorized resolvers
  - Notify if excessive name resolution errors occur
- Examine critical data for “correctness” at DNS zone data and recursor caches
- Use Passed DNS replication to
  - Review what names your users are resolving
  - Populate Resource Policy Zones, domain blocklists

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