AMRES
Serbian Academic Network

BELGRADE SECURITY WORKSHOP 2015

# Improving DNS security and reliability

Jean BENOIT, University of Strasbourg / RENATER Campus Best Practice

UNIVERSITÉ DE STRASBOURG

RENATER
CONNECTEUR DE SAVOIRS

GÉANT

# Introduction

- Best practice about DNS
  - Not about DNSSEC
  - Mostly old stuff : other DNS best practice documents have been written before...
- How was this one written ?
  - Operational experience of running DNS for several years for tens of thousands of users
  - Compilation of several documents
- Geant / RENATER CBP document
- Authors :
  - Olivier PRINS (CNRS), Jean BENOIT (University of Strasbourg)

# Outline

- General recommandations
- Securing DNS data in an authoritative DNS
- Securing recursive resolution service

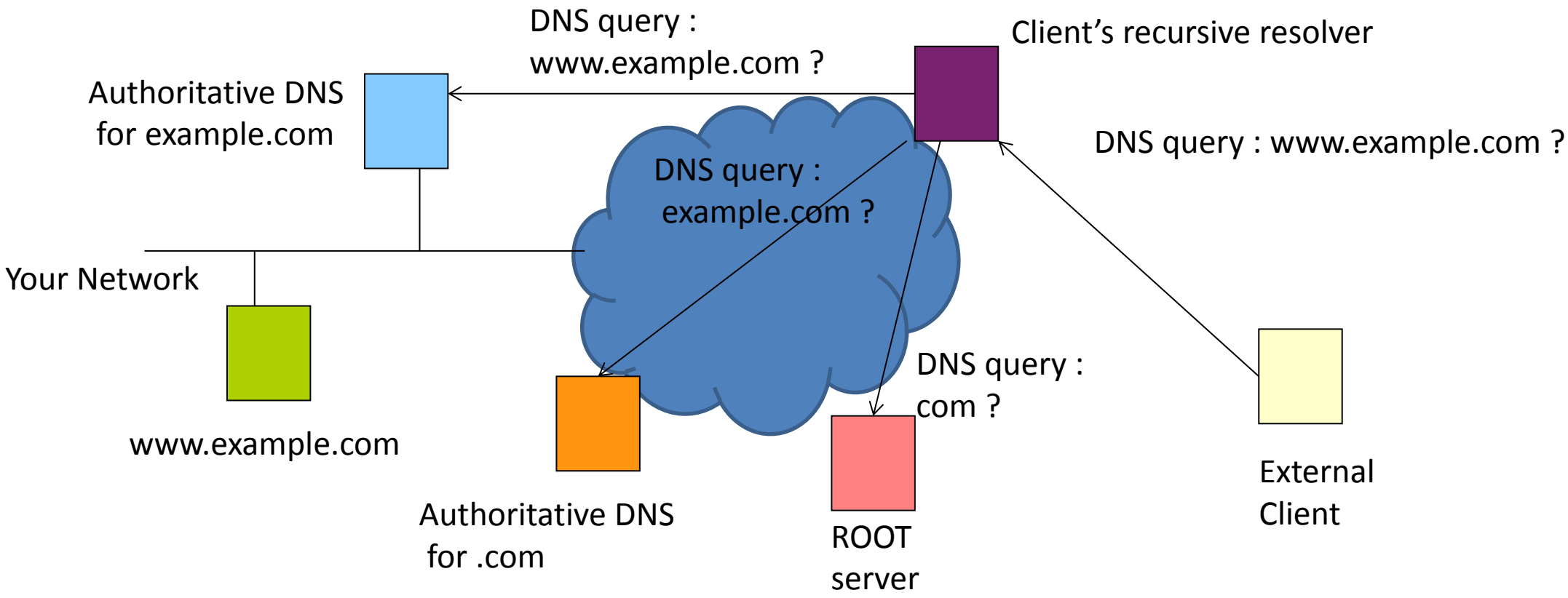
# Outline

- General recommandations
- Securing DNS data in an authoritative DNS
- Securing recursive resolution service

# General recommendations

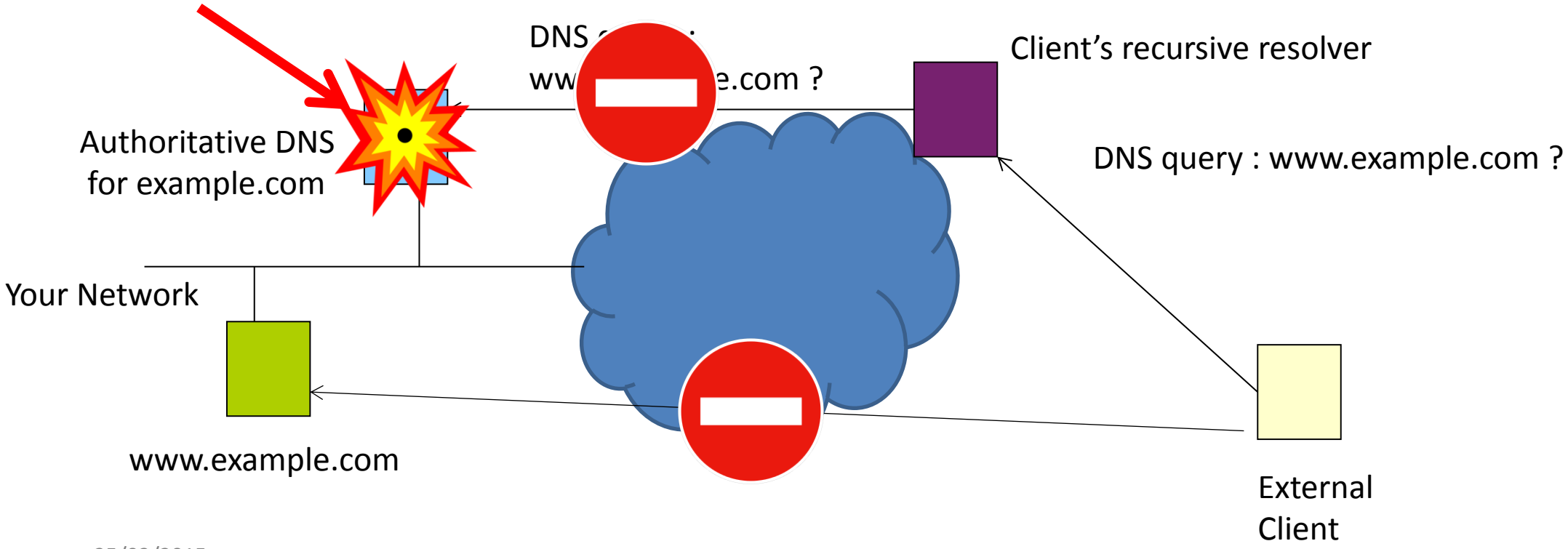
- 2 types of Domain Name Services
  - authoritative server
    - Master
    - Slaves
  - recursive resolution
- 2 types of data
  - public zones
  - private zones

# Recursive resolution and authoritative server



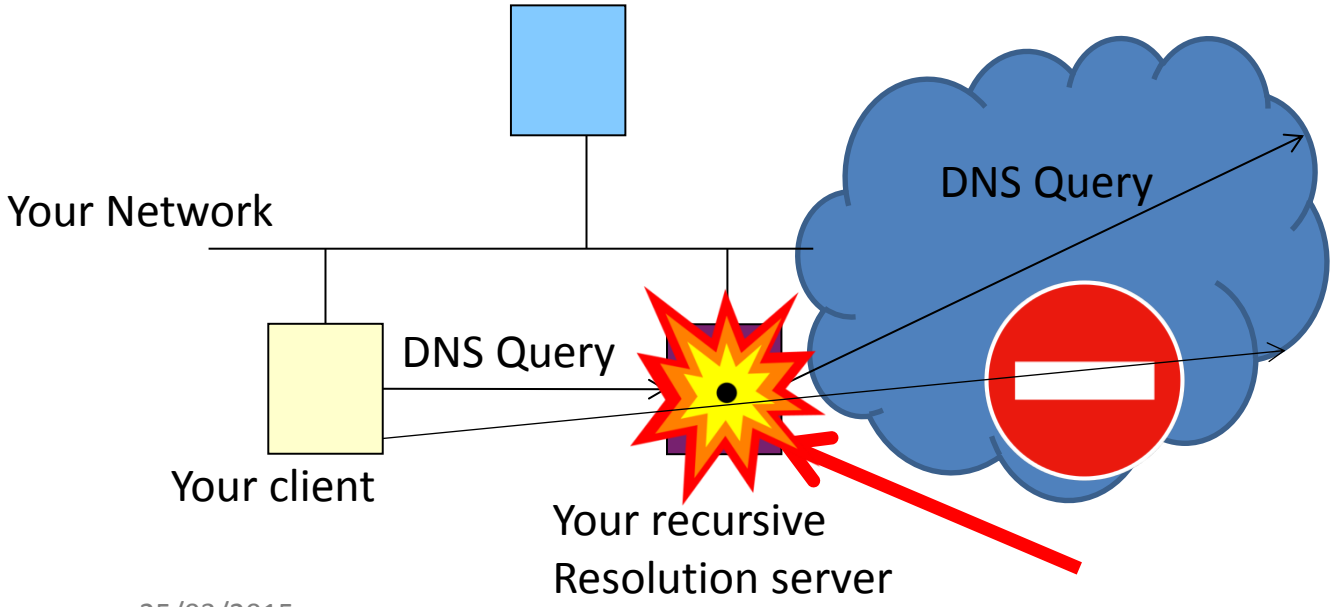
# Authoritative server

- Used by external users to reach your resources
- no authoritative DNS for a long time → no access to your web site from the outside



# Recursive resolution

- Used by **your** users
- Server doing the recursive resolution puts answers in a cache
- It is a critical service : no recursive resolution → no network access for your users



# Recursive/authoritative separation

- Best practice to separate
  - recursive resolution service

  and
  - authoritative server
- if authoritative server is down, your users can still access the internet
- if recursive resolution service is down, internal resources still accessible from the outside

# Diversity→resiliency

- For one master authoritative server, have multiple slave servers
- Put your servers on different networks
  - different subnets, AS, different geographical sites
- Use different software implementations :
  - Bind, Unbound, NSD, Knot etc.
  - Running on different OS (Linux, BSD, etc.)

# Outline

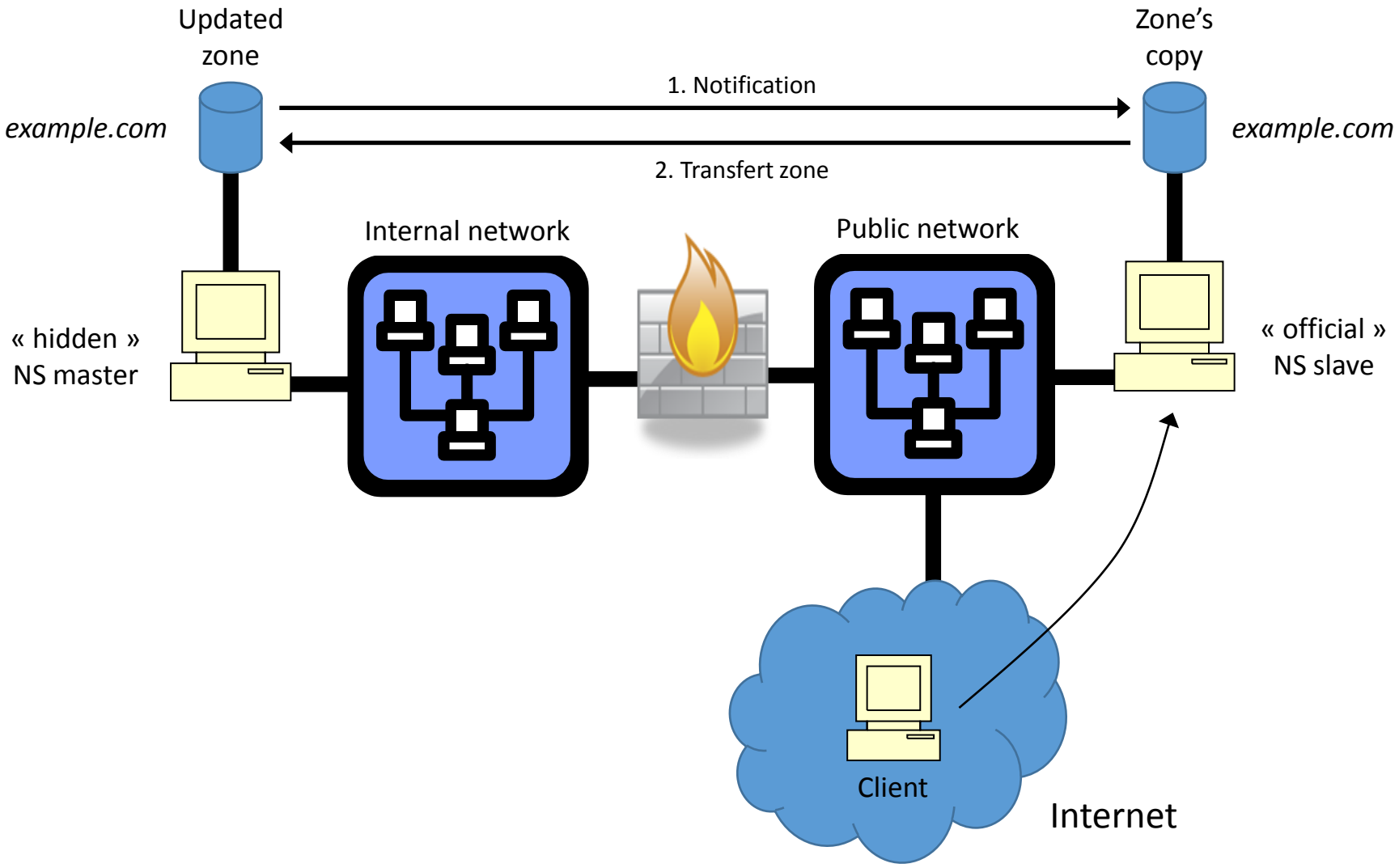
- General recommandations
- Securing DNS data in an authoritative DNS
- Securing recursive resolution service

# Major risk: master DNS compromission

- Major risk: compromission of your DNS data
- If the zones are modified on the master server

  → all the slaves will serve the modifications
- DNSSEC can protect you from some form of DNS data modifications
  - Query results can be validated with DNSSEC
  - DNSSEC is strong against DNS cache poisoning
  - But DNSSEC is not widely deployed yet
  - If your authoritative server is compromised, your keys may also be compromised, depending on how you handle the keys

# Stealth or hidden master



# Split-DNS (Views)

- Protecting private zones
  - Internal hosts names and address
- Send data depending on source IP address of the host asking for it
  - Serve public information to outside hosts
  - Serve private informations to internal hosts

# How to securely modify your DNS data ?

- 1st option: by hand
- Edit zone file with a text editor
- Use checking tools to avoid syntax errors

# How to securely modify your DNS data ? Automated editing

- 2nd option: automation
- IPAM: IP Address Management = Database + CLI/Web interface
  - Example: Netmagis
- Modify records in IPAM→ automatic zone file generation
- Less error prone, forward/reverse record consistency
- Easy to migrate to another DNS software (change zone generation code)
- Delegate rights to modfiy to other admins
- Apply policies : consistent naming scheme
- Other automations easy (mass declaration or renaming)

# How to securely modify your DNS data ?
# Automated editing

- Usual risks of automation
- Complexity: more elements to handle (DB, web, authentifcation, generation tools)
- Difficult to debug
- Security flaw in the tool → data modifications
- You must secure the access to the tool

# Outline

- General recommandations
- Securing DNS data in an authoritative DNS
- Securing recursive resolution service

# Interactions with authoritative resolver

- Interactions exist between

  your own recursive resolution service /

  your authoritative resolver
- Separating recursive/authoritative breaks a few things
- Recursive resolver queries your authoritative server: cache sync problem
  - How to trigger cache flush on recursive resolution server when master changes ?
  - No access to private zones for your hosts:

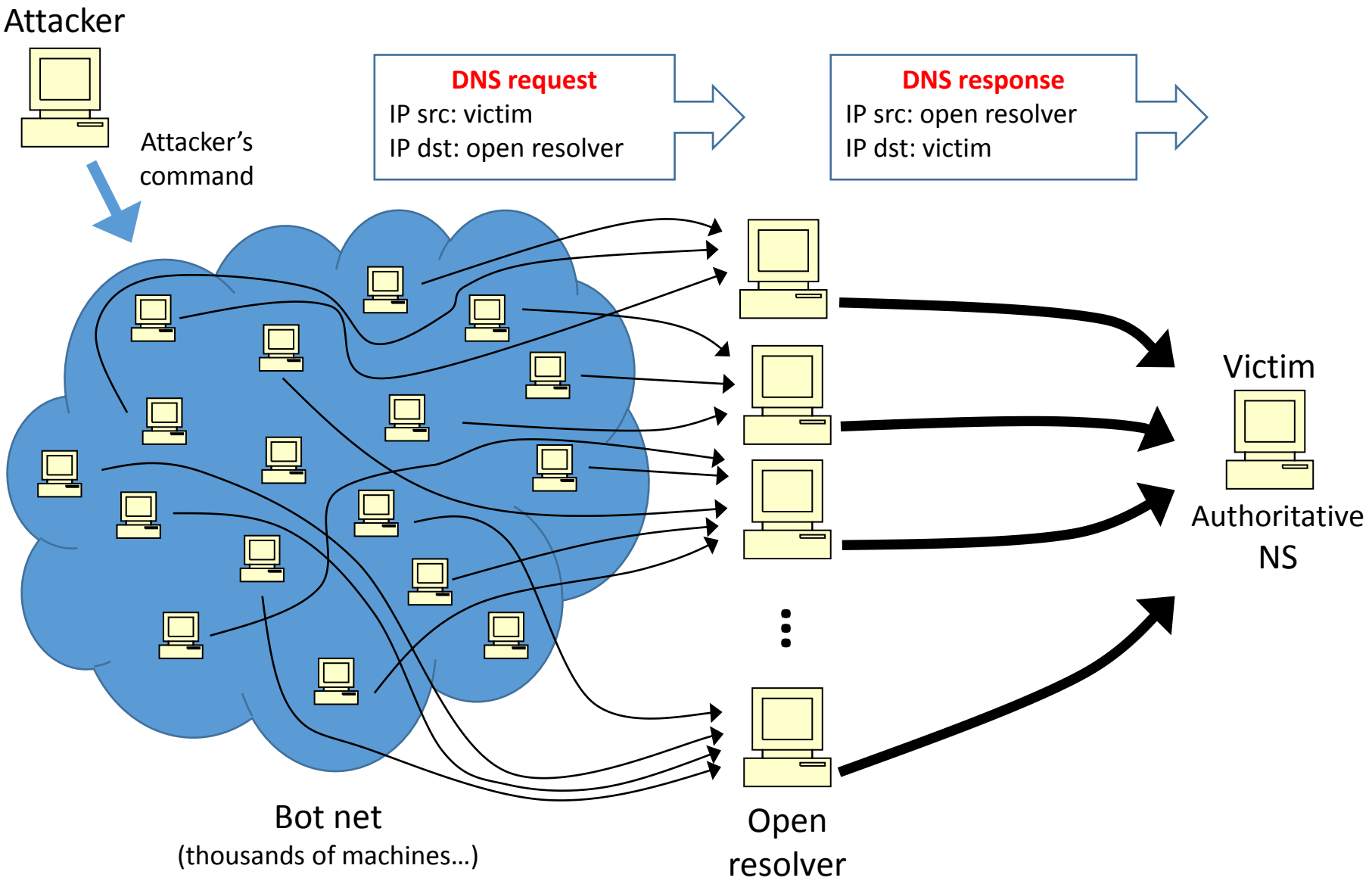
    Explicit configuration directive in recursive resolution server

    myzone.local → internal authoritative server IP address

# Recursive resolution service redundancy

- Different approaches to a resilient design
- Anycast DNS (BGP)
- Generic redundancy protocol (VRRP)

# DDoS attacks through open resolvers



# Open resolvers

- any hosts with an open recursive resolution service can be a vector in a DDoS attack by amplification
- Best Practice: filter external access to all DNS that allow recursion
  - Allow DNS traffic from/to official DNS servers
- Rate-limiting

# BELGRADE SECURITY WORKSHOP 2015