Domain Name System (DNS) and DNS Security

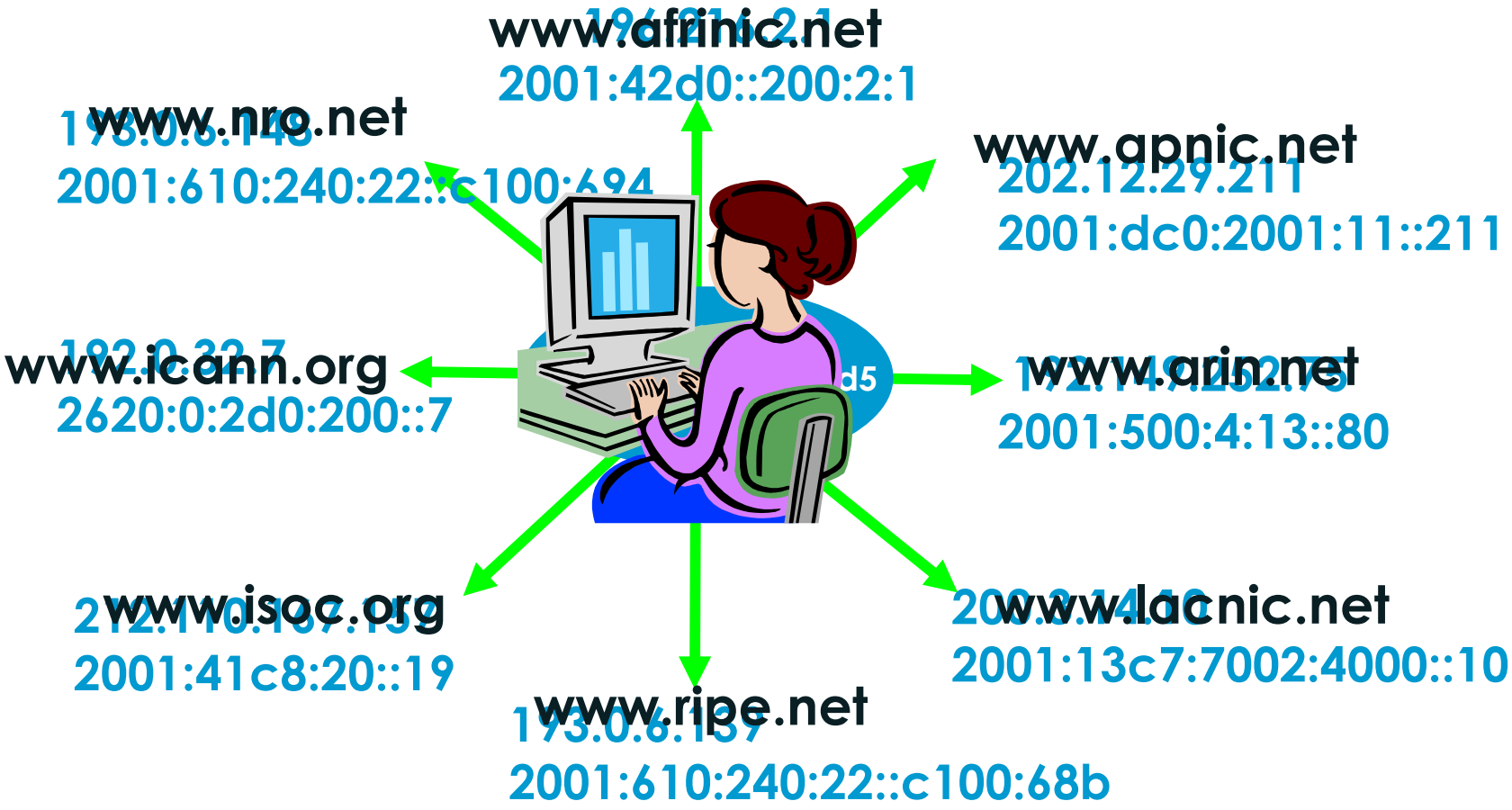
Jia-Rong Low | Vice President and Managing Director
Asia Pacific, ICANN

Asia Pacific Internet Governance Academy 2017
August 2017

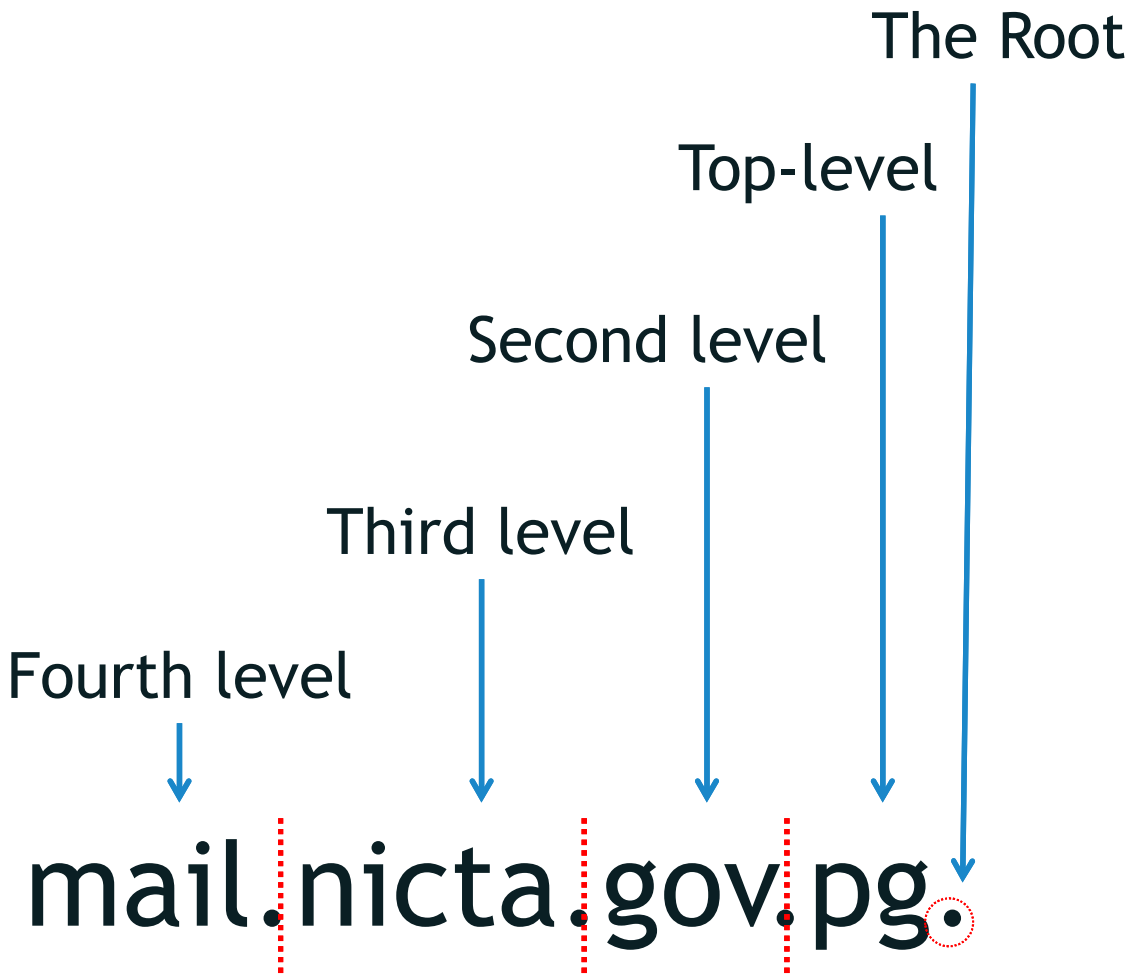
Unique Identifiers

- Names
- Numbers
- Protocol Parameters

Names – Easier way for humans

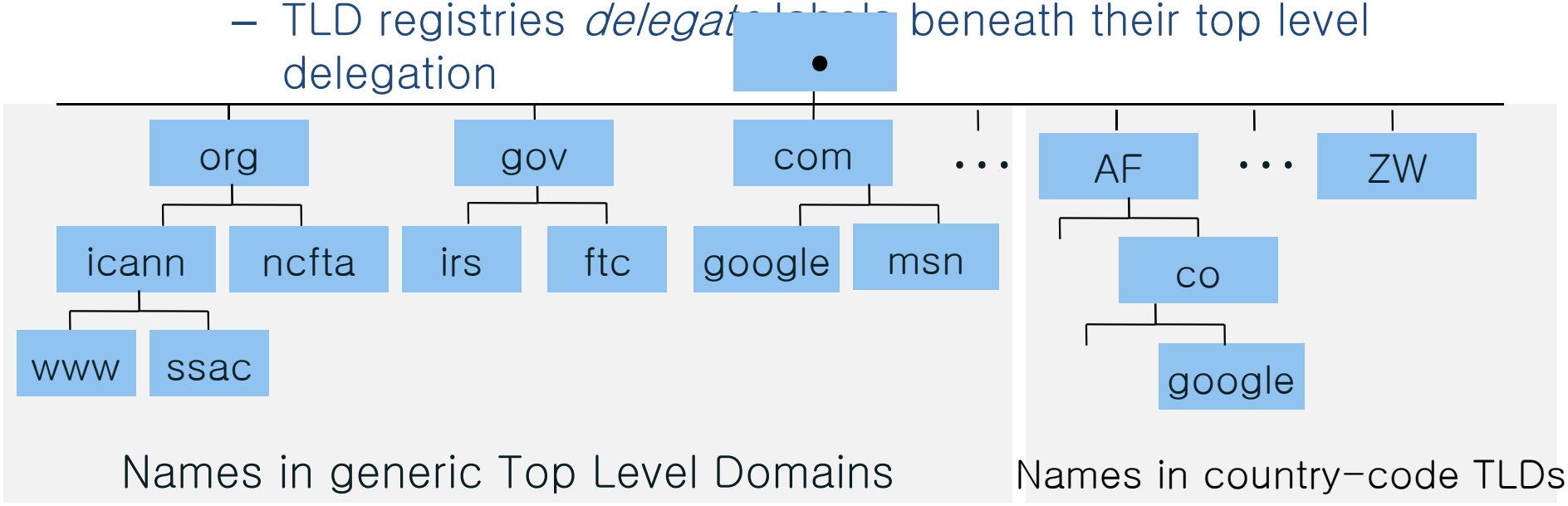


Domain Name's Structure

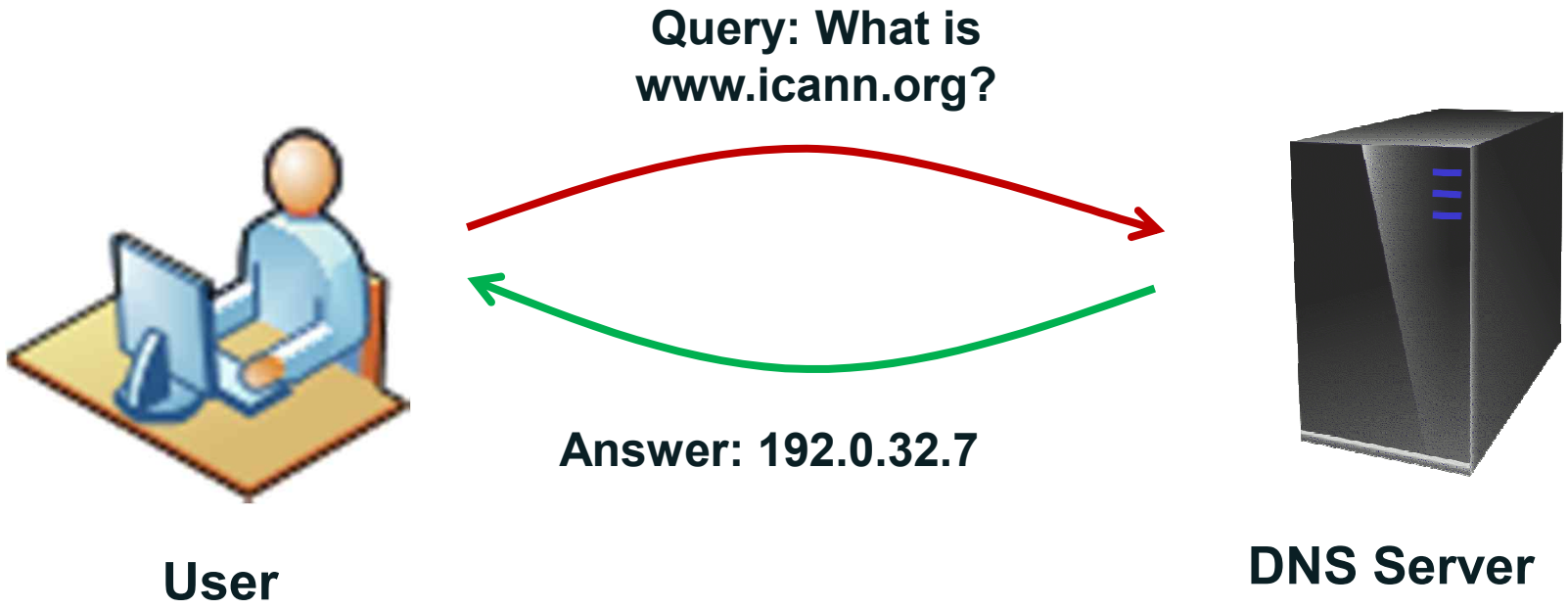


DNS Structure

- A **domain** is a node in the Internet name space
  - A domain includes all its descendants
- Domains have names
  - Top-level domain (TLD) names are generic or country-specific
  - TLD *registries* administer domains in the top-level
  - TLD registries *delegat* beneath their top level delegation



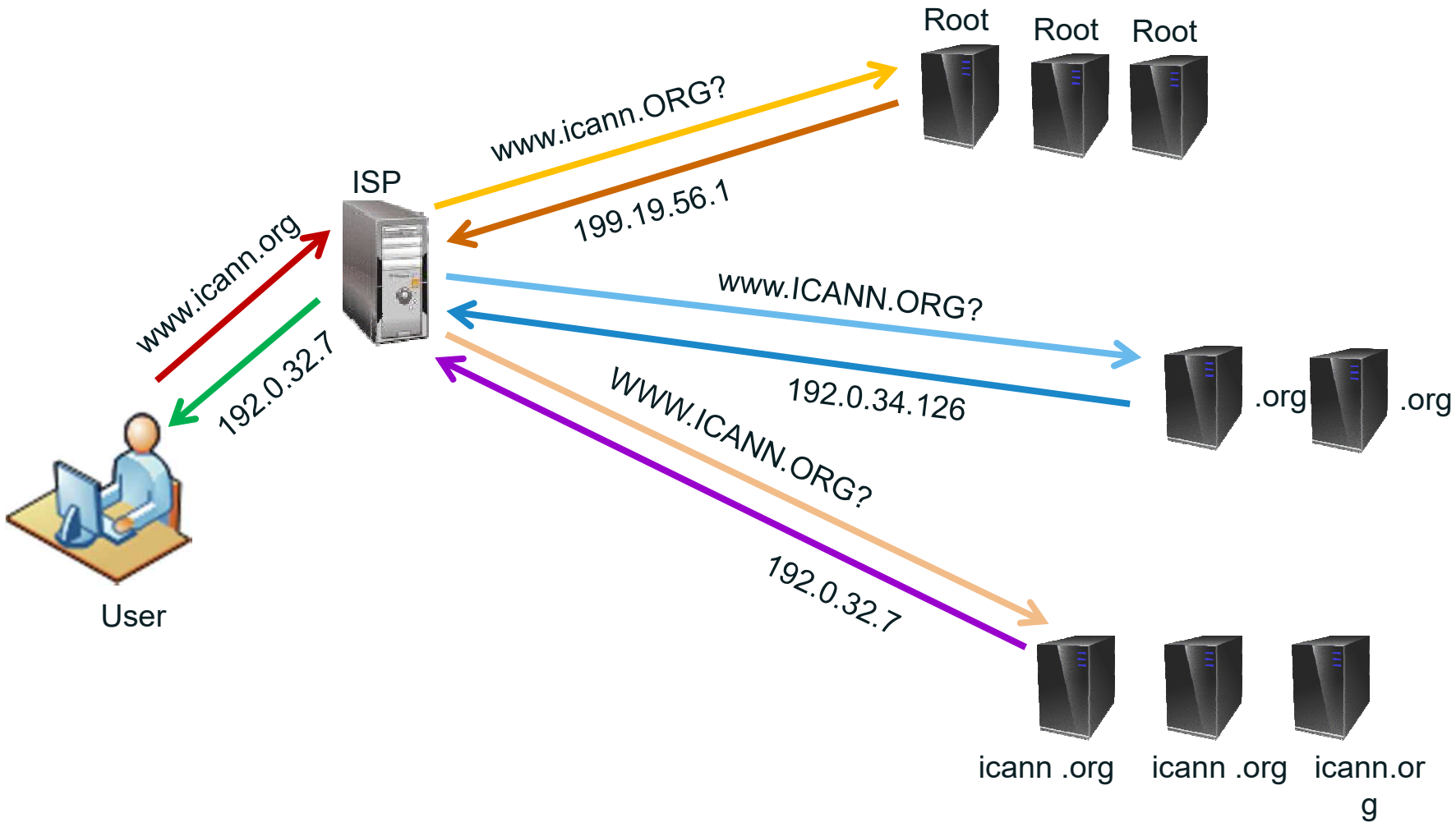
DNS Operation



DNS Resolution

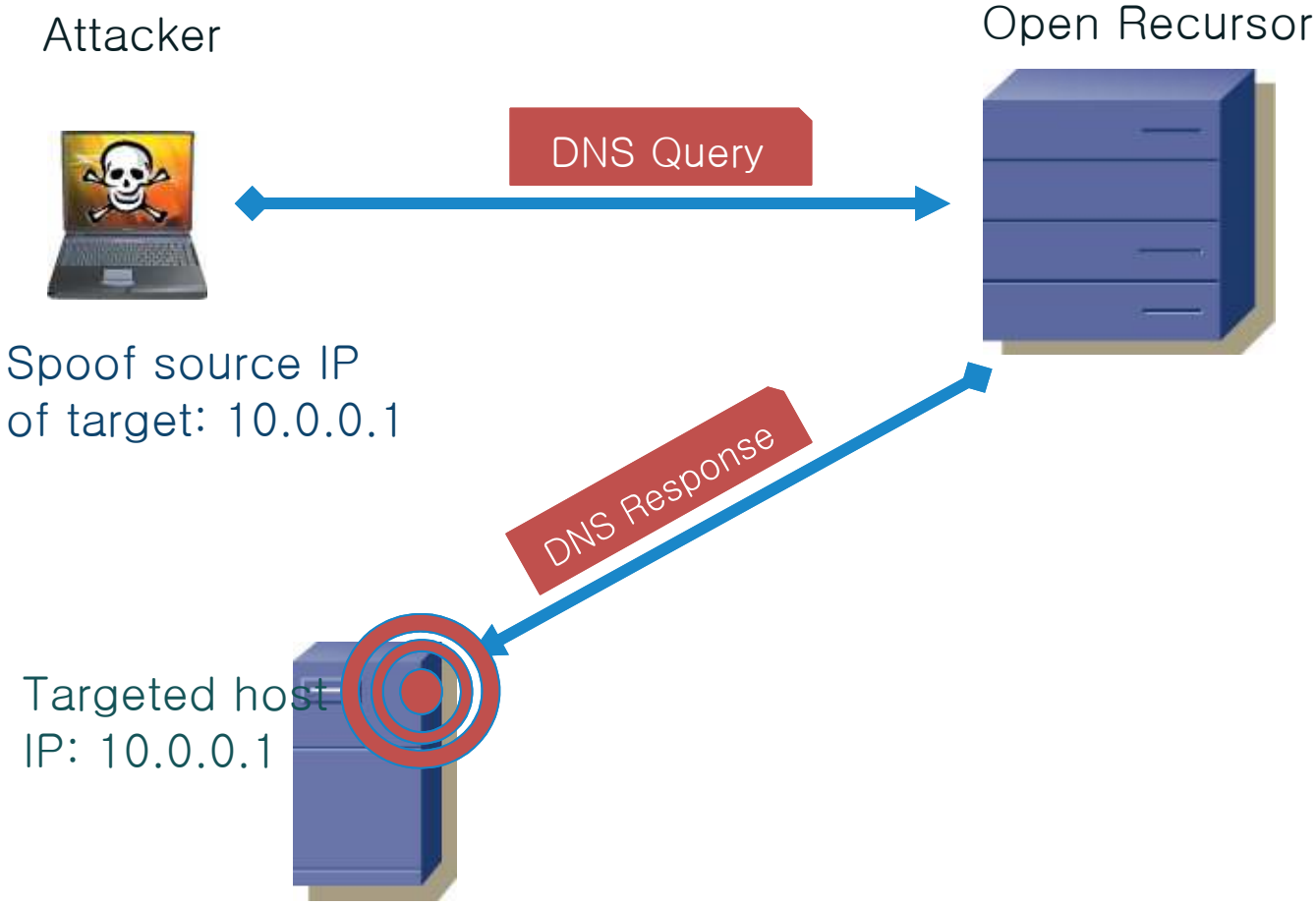
Role Play

DNS Operation



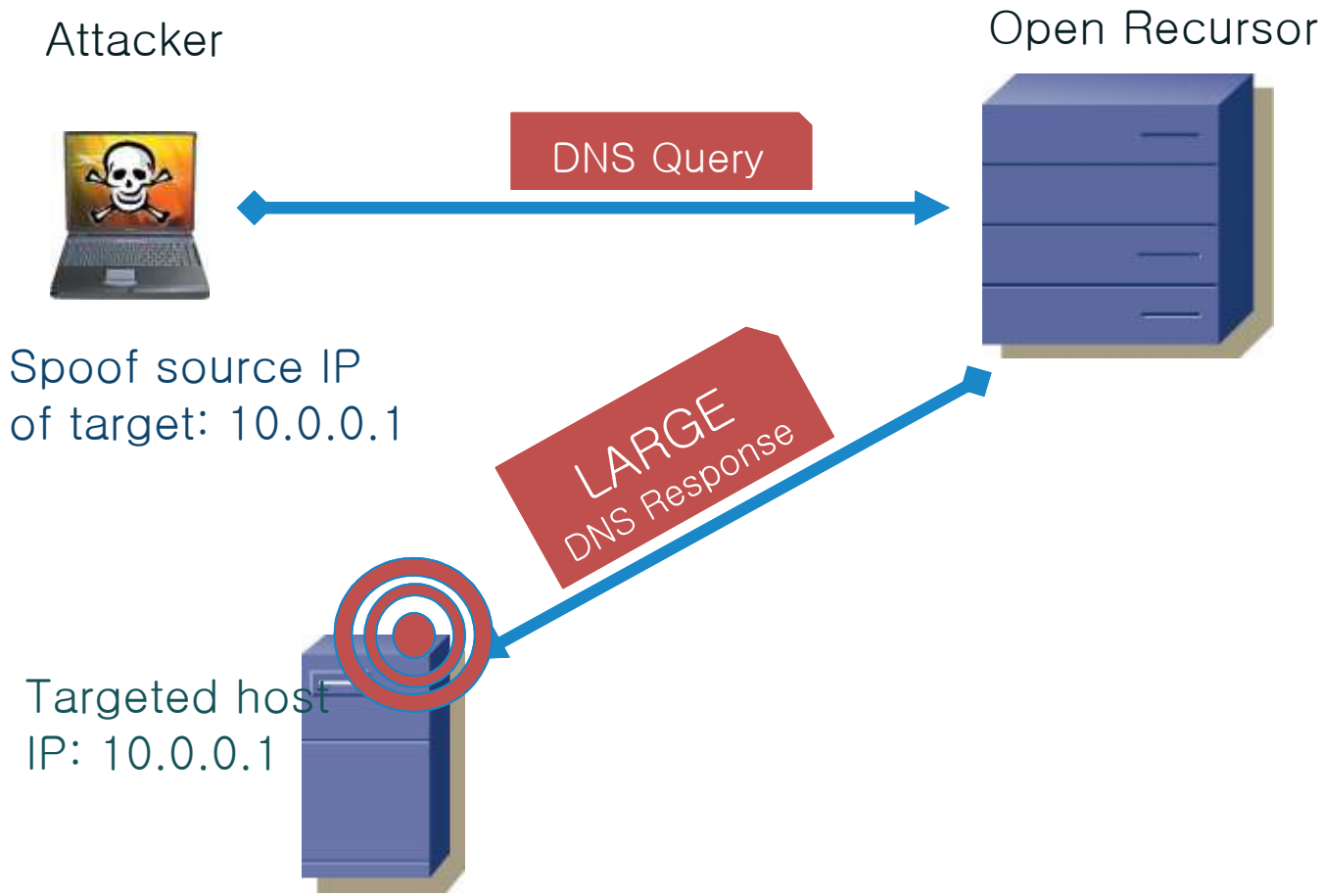
DNS Security

Reflection attack



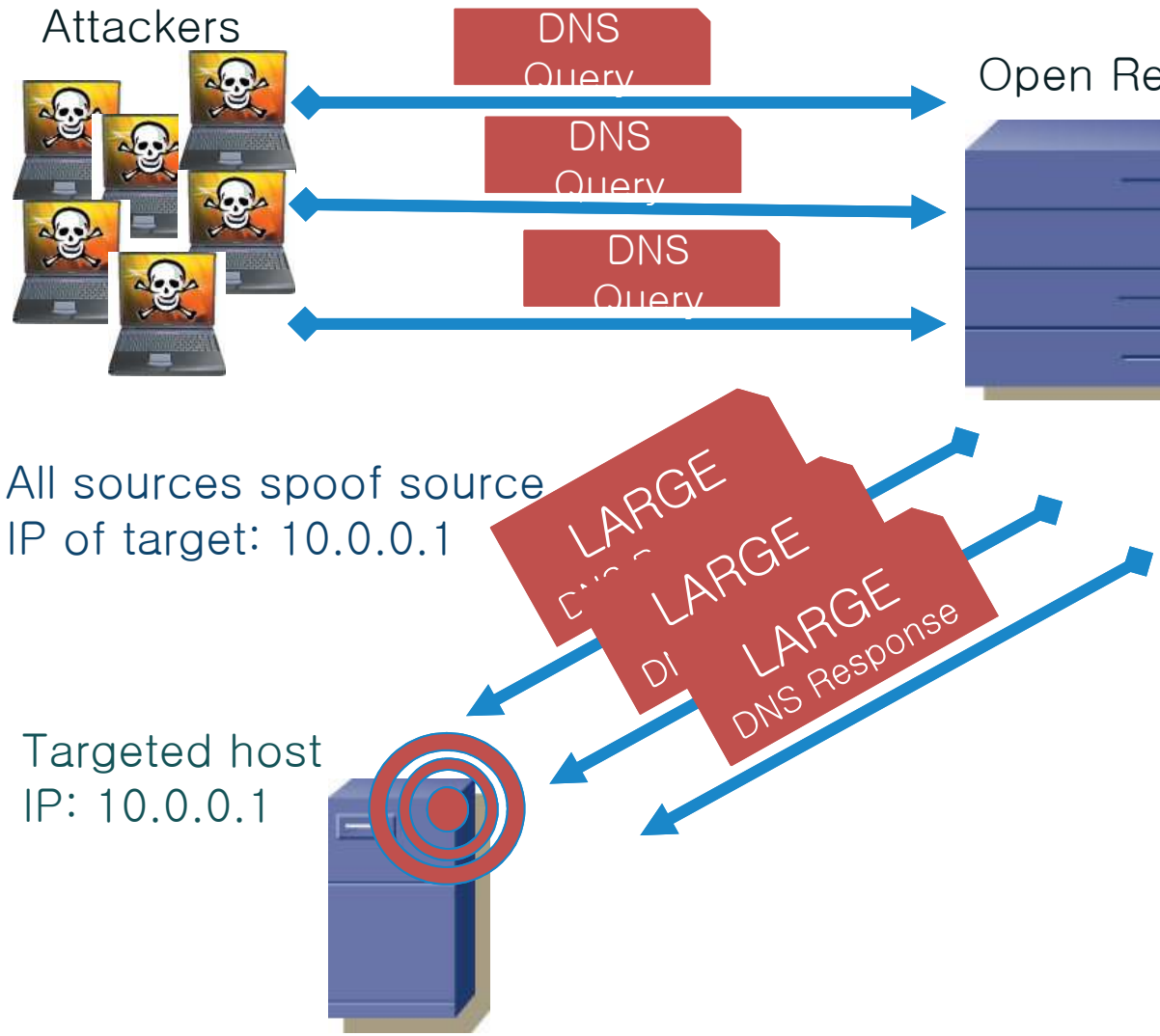
- Attacker sends DNS messages to recursor from spoofed IP address of target
- Recursor sends response to targeted host
- Response delivered to targeted host

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)



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

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

My Mac

What is the IPv4 address for loseweightfastnow.com

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

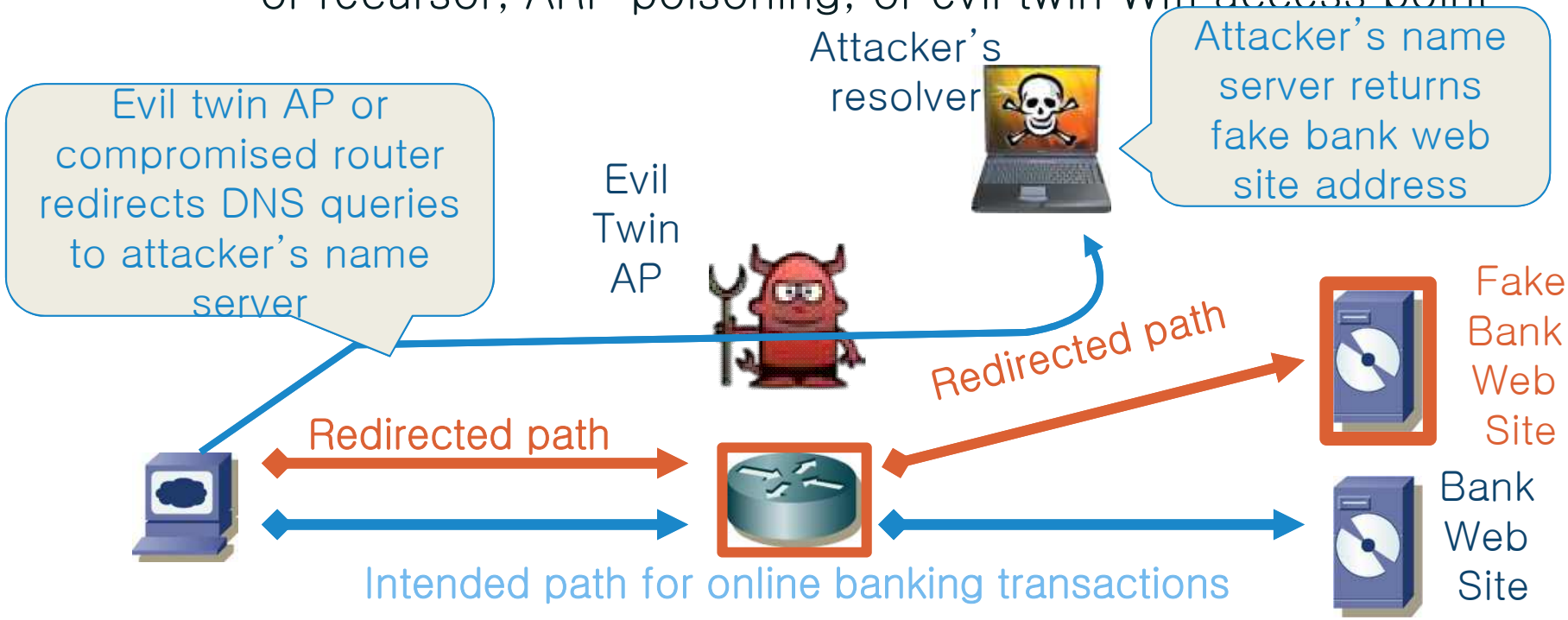
My local resolver

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

ecrime name server

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



Securing DNS

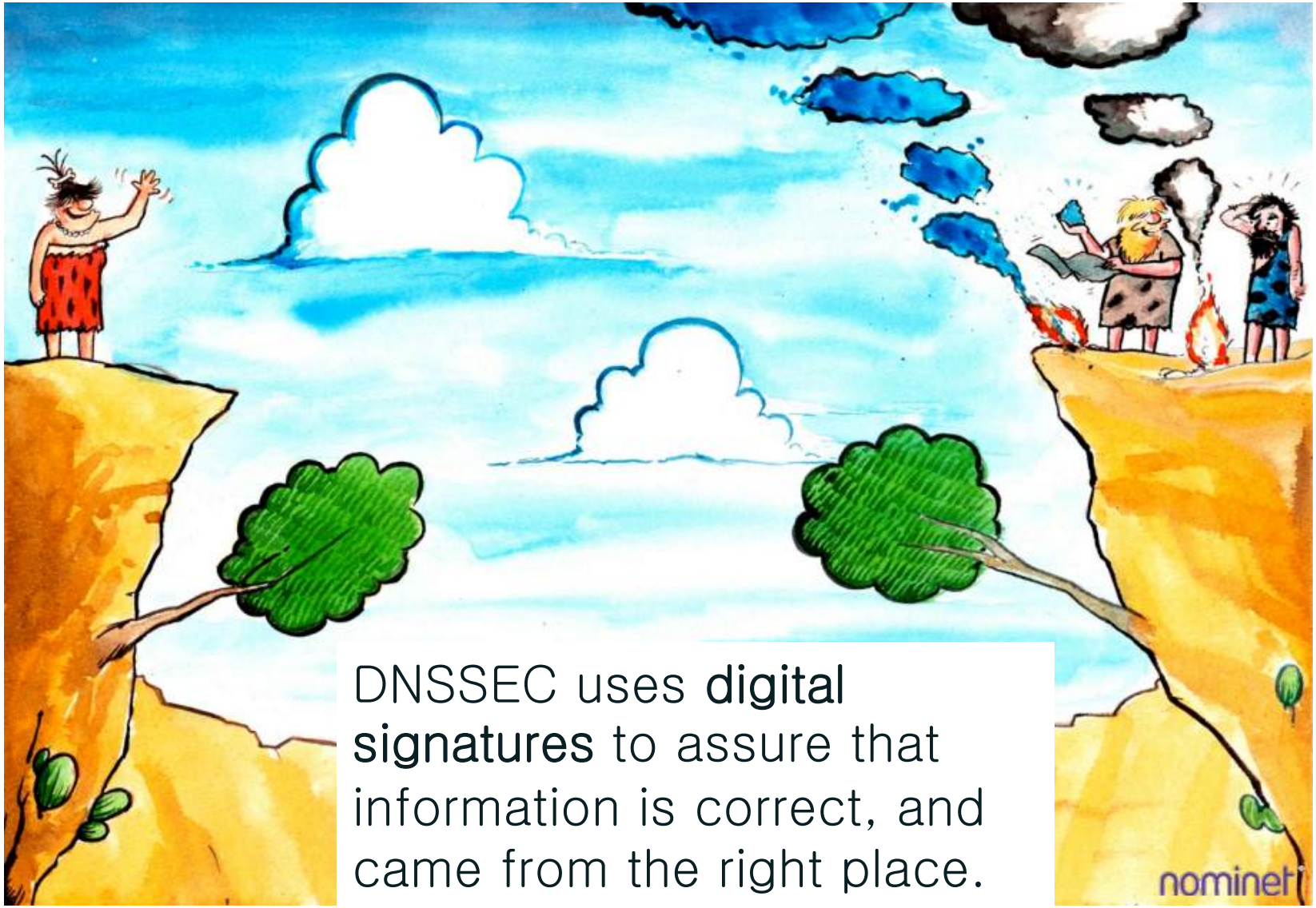
- There are two aspects when considering DNS Security
  - Server protection
  - Data protection
- Server protection
  - Protecting servers
    - Make sure your DNS servers are protected (i.e. physical security, latest DNS server software, proper security policies, Server redundancies etc.)
  - Protecting server transactions
    - Deployment of TSIG, ACLs etc. (To secure transactions against server impersonations, secure zone transfers, unauthorized updates etc.)
- Data protection
  - Authenticity and Integrity of Data
    - Deployment of DNSSEC (Protect DNS data against cache poisoning, cache impersonations, spoofing etc.)

DNS Security Extensions (DNSSEC)

DNSSEC – simplified

DNSSEC – simplified

DNSSEC – simplified



What is DNSSEC?

- DNSSEC = **“DNS Security Extensions”**
- DNSSEC is a protocol that is currently being deployed to secure the Domain Name System (DNS)
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names
- Result of over a decade of community based, open standards development