Naming
Domain Name System

Guevara Noubir

Fundamentals of Computer Networks

Northeastern University

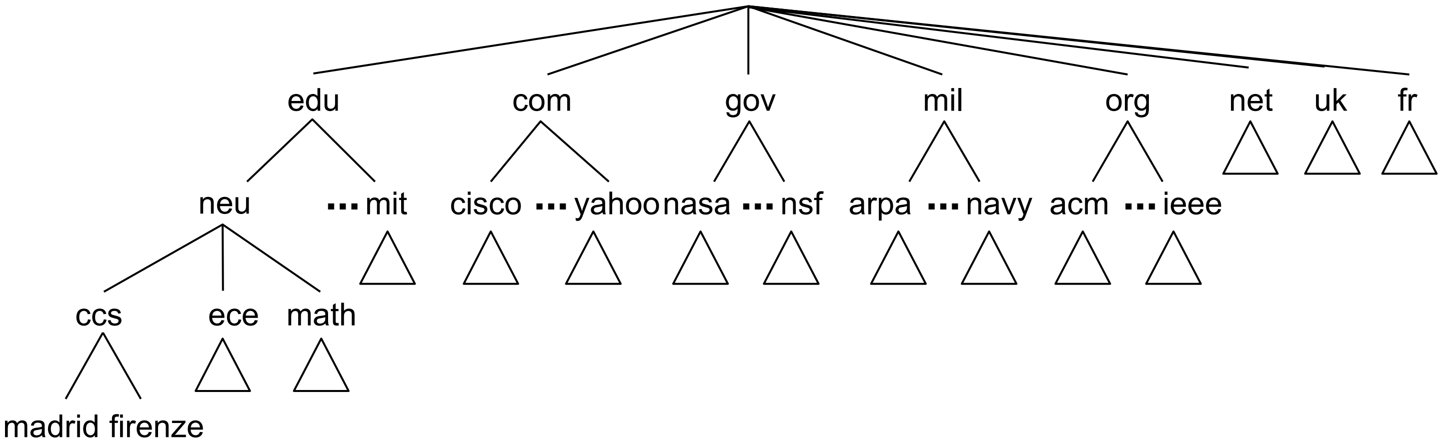
Domain Name System

- DNS is a fundamental application layer protocol

- Not visible but invoked every time a remote site is accessed

Domain Naming System

- Hierarchy

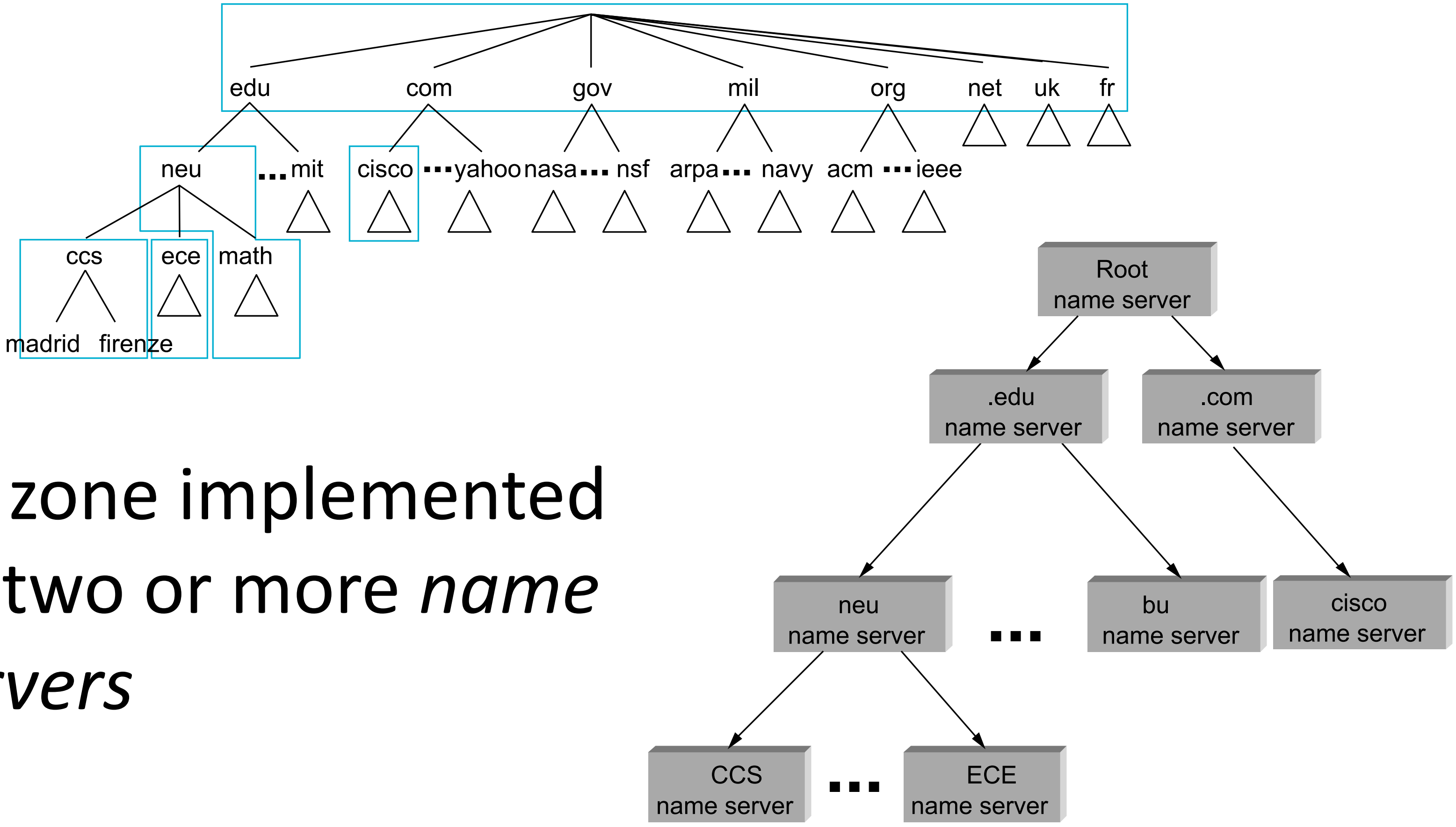


- DNS maps abstract names to specific resources

```
madrid.ccs.neu.edu -> 129.10.112.229
```

Name Servers

- Partition hierarchy into *zones*



Each zone implemented by two or more *name servers*

Resource Records

- Each name server maintains a collection of *resource records*
  `(Name, Value, Type, Class, TTL)`
- Name/Value: not necessarily host names to IP addresses
- Type
  - A: Value is an IP address
  - NS: Value gives domain name for host running name server that knows how to resolve names within specified domain
  - CNAME: Value gives canonical name for particle host; used to define aliases
  - MX: Value gives domain name for host running mail server that accepts messages for specified domain
  - TXT: additional text info
  - SPF: Sender Policy Framework
- Class: allow other entities to define types
  - IN: Means Internet
- TTL: how long the resource record is valid

.edu Server

```
(neu.edu, nb4276.neu.edu, NS, IN)
(nb4276.neu.edu, 155.33.16.201, A, IN)
```

neu.edu Server

```
(neu.edu, nb4286.neu.edu, MX, IN)
(ccs.neu.edu, amber.ccs.neu.edu, NS, IN)
(amber.ccs.neu.edu, 129.10.116.51, A, IN)
(ece.neu.edu, ns1.ece.neu.edu, NS, IN)
(ns1.ece.neu.edu, 129.10.60.31, A, IN)
(mystic.math.neu.edu, 129.10.75.101, A, IN)
```

ccs.neu.edu Server

```
(ccs.neu.edu, amber.ccs.neu.edu, MX, IN)
(amber.ccs.neu.edu, 129.10.116.51, A, IN)
(ccs.neu.edu, atlantis.ccs.neu.edu, MX, IN)
(atlantis.ccs.neu.edu, 129.10.116.41, A, IN)
```

Name Resolution

- To reach firenze.ccs.neu.edu

- Strategy
  - Go to local name server
  - Local name server goes to root name server
  - Local name server goes to edu name server
  - Local name server goes to neu.edu name server
  - Local name server goes to ccs.neu.edu name server and gets IP address

DNS Cache Poisoning

- DNS servers cache information
- Poisoning an ISP DNS cache impacts all the ISP users
- How?
  - Attacker queries the ISP DNS server
  - ISP DNS Server starts resolving the query by asking the authoritative name server
  - Attacker simultaneously sends a DNS response spoofing the IP address of the authoritative name server and providing a malicious IP address
  - All the ISP users will be directed to the attacker sites
- Problems?

DNS Cache Poisoning with Birthday Paradox Technique

- Randomization makes it hard to predict the transaction ID (16 bits)
- Attacker sends *n* fake requests and spoofs *n* malicious replies
- Probability of failing to match at least one query is:
  - $P_{fail} = (1-n/2^{16})^n$
  - If $n = 213 \Rightarrow P_{fail} < 0.5$
- Problems?

Subdomain DNS Cache Poisoning (2008)

- Attacker generates requests for non-existing sub-domains
  - e.g., non-existing.example.com
- The name server for the target domain ignores the requests
- The attacker issues spoofed responses with guessed transaction ID (no competition from target domain)
- Attacker response includes a response that resolves the name server of that target domain e.g., example.com to a malicious IP address
- Was successful against many DNS software packages e.g., BIND

Client-Side DNS Cache Poisoning

- Attacker sets up a malicious website
- Webpage contains HTML tags that automatically issue requests for additional URLs e.g., image tags with non-existing subdomains of the target domain
- The attacker knows when to start spoofing the DNS replies because he owns the malicious website

- Current solutions:
  - Source port randomization
  - Limiting ISP DNS replies to internal requests
  - DNSSEC

DNSSEC

- DNS was not designed with security in mind
- DNSSEC provides a crypto-based solution that extends DNS (RFC 2535)
- Since 2000 but only slowly being deployed
- DNSSEC adds new types of DNS records
- DNS query:
  - Client indicates that DNSSEC is supported
- DNS reply:
  - If server supports DNSSEC, RRSIG digital signature is included

- Issues:
  - PKI infrastructure / chain of trust following domain name hierarchy
  - Root name server does not support DNSSEC
  - Performance

Summary

- Domain Name System is a critical application of the Internet
  - e.g., it also enables Content Delivery Networks
- Major flaws have been identified and partially fixed
- A strong solution (DNSSEC) is slowly being deployed (typical problem with the Internet)