DNS
Lecture 12

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

August 12, 2021

Source of some slides: **Princeton University**, **Cornell University**, and **Stanford University**

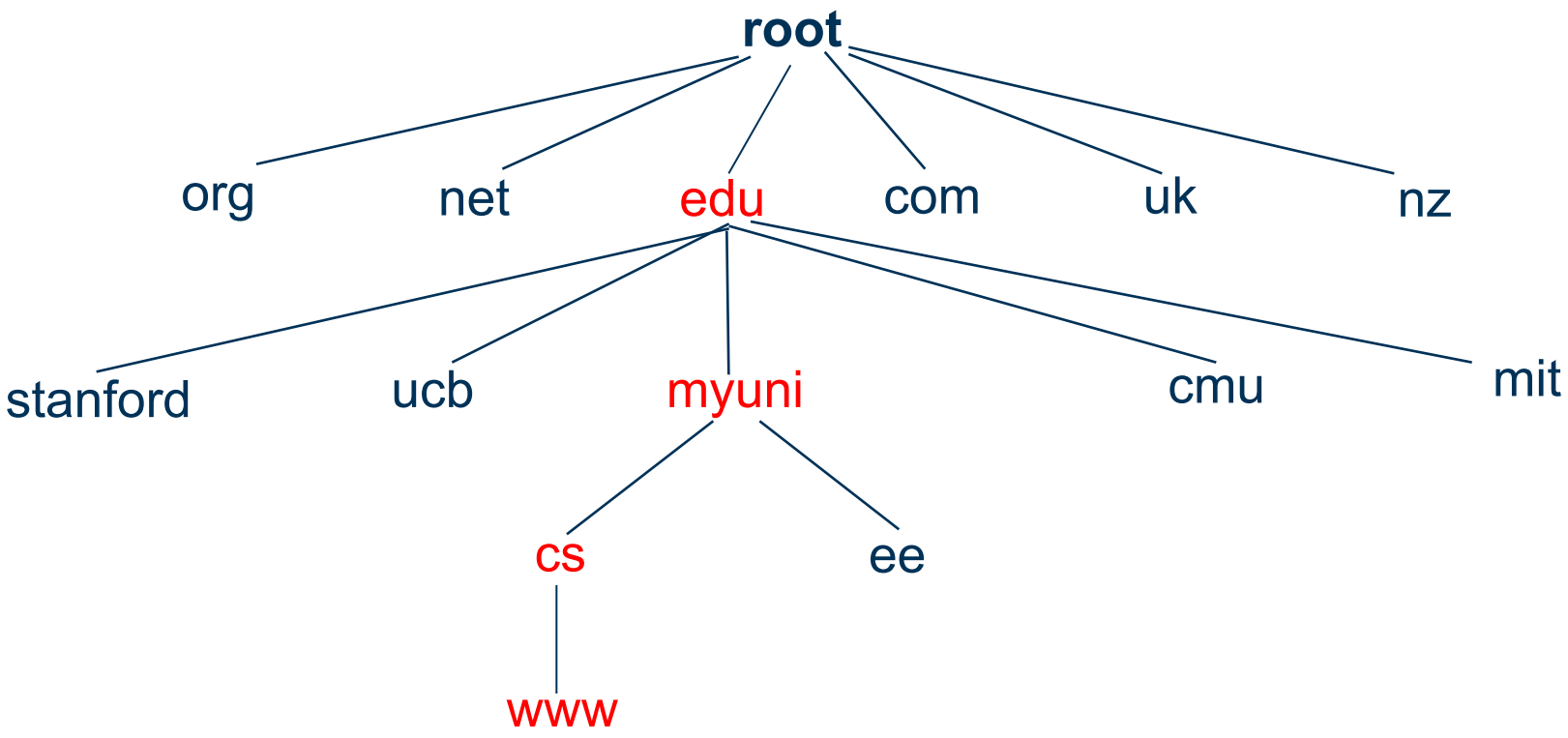
HOSTNAME VS IP ADDRESSE

- Host names
  - Mnemonic name appreciated by humans
  - Variable length, alphanumeric characters
  - Examples: www.cnn.com and nzherald.co.nz
- IP addresses
  - Numerical address processed by routers
  - Fixed length, binary number
  - Hierarchical, related to host location
  - Examples: 64.236.16.20 and 193.30.227.161

DOMAIN NAME SYSTEM (DNS)

- Properties of DNS
  - Hierarchical name space divided into zones
  - Distributed over a collection of DNS servers
- Hierarchy of DNS servers
  - Root DNS servers
  - Top-Level Domain (TLD) DNS servers
  - Authoritative DNS servers
- For performing translations
  - Local DNS servers
  - Resolver software (client end)

HIERARCHICAL NAME SPACE



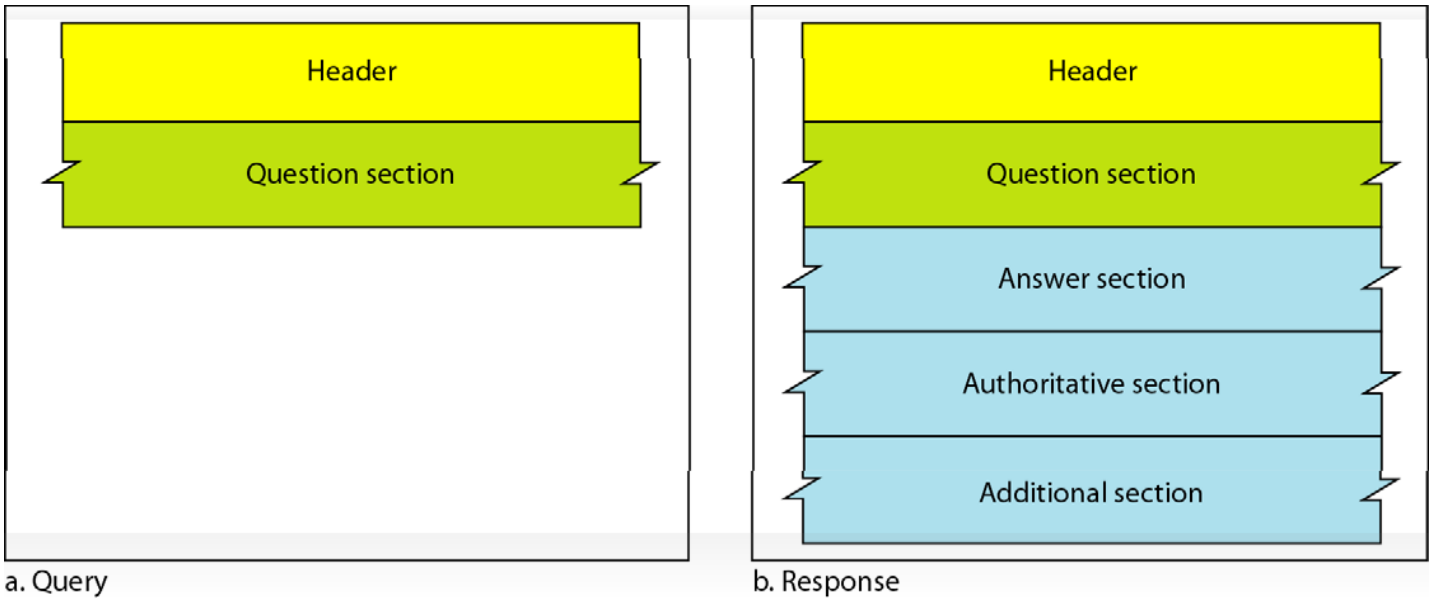
AUTHORITATIVE VS NON-AUTHORITATIVE ANSWER

- An authoritative answer from a name server is “guaranteed” to be accurate

- A non-authoritative answer may not be accurate
  - Such as an answer from the cache

DNS PROTOCOL

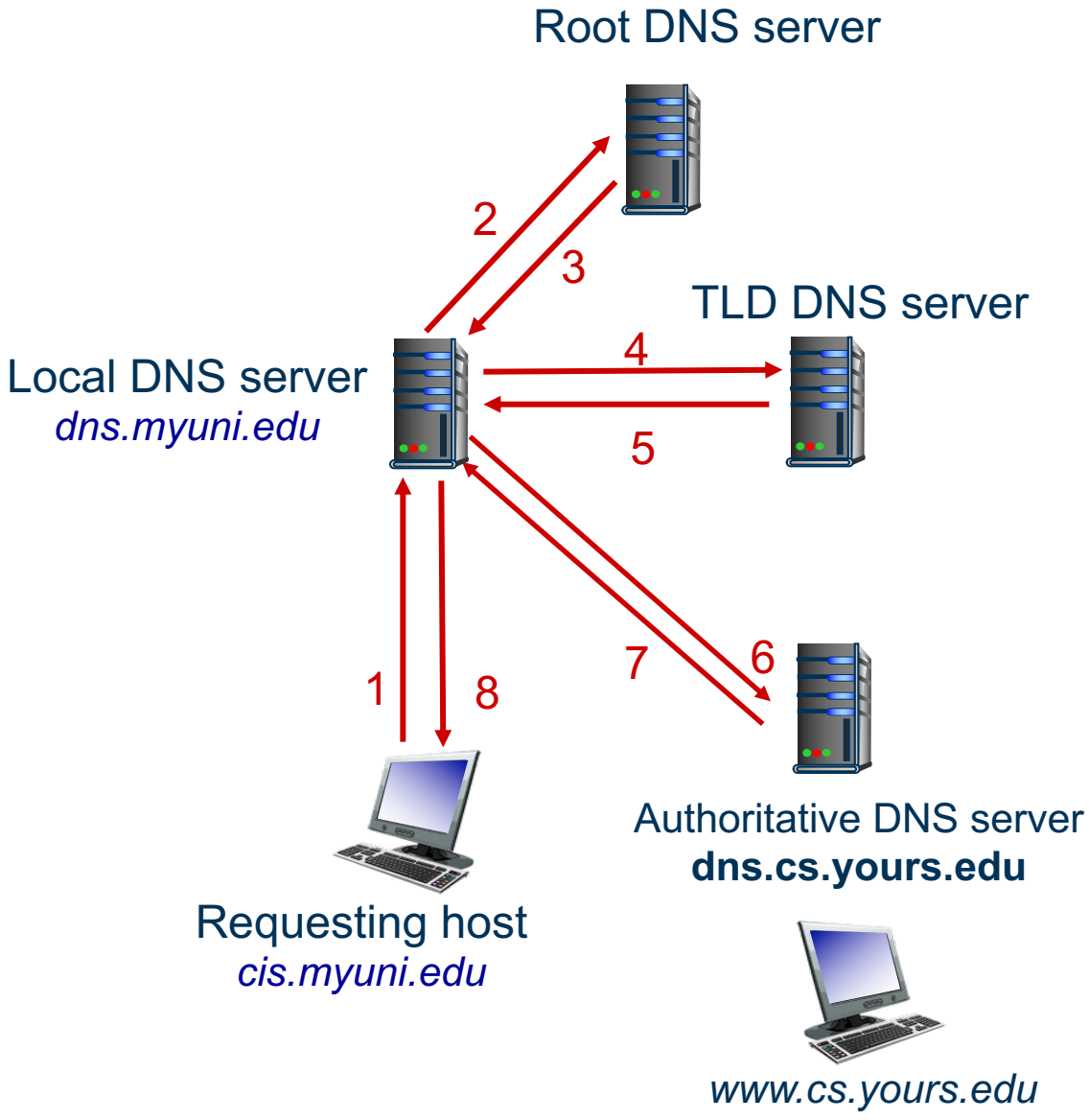
- DNS has two types of messages: Query and response
- 16-bit random value links response to a query ID



a. Query

b. Response

DNS RESOLUTION



DNS RESOURCE RECORD (RR)

- RR format
  - (Name, value, type, TTL)
- Name and value for hostname and IP address
- Type
  - **A** means hostname
  - **NS** means name server
  - **M** means canonical name
  - **MX** means mail server
- TTL (Time To Live)
- There may be multiple records returned for one query

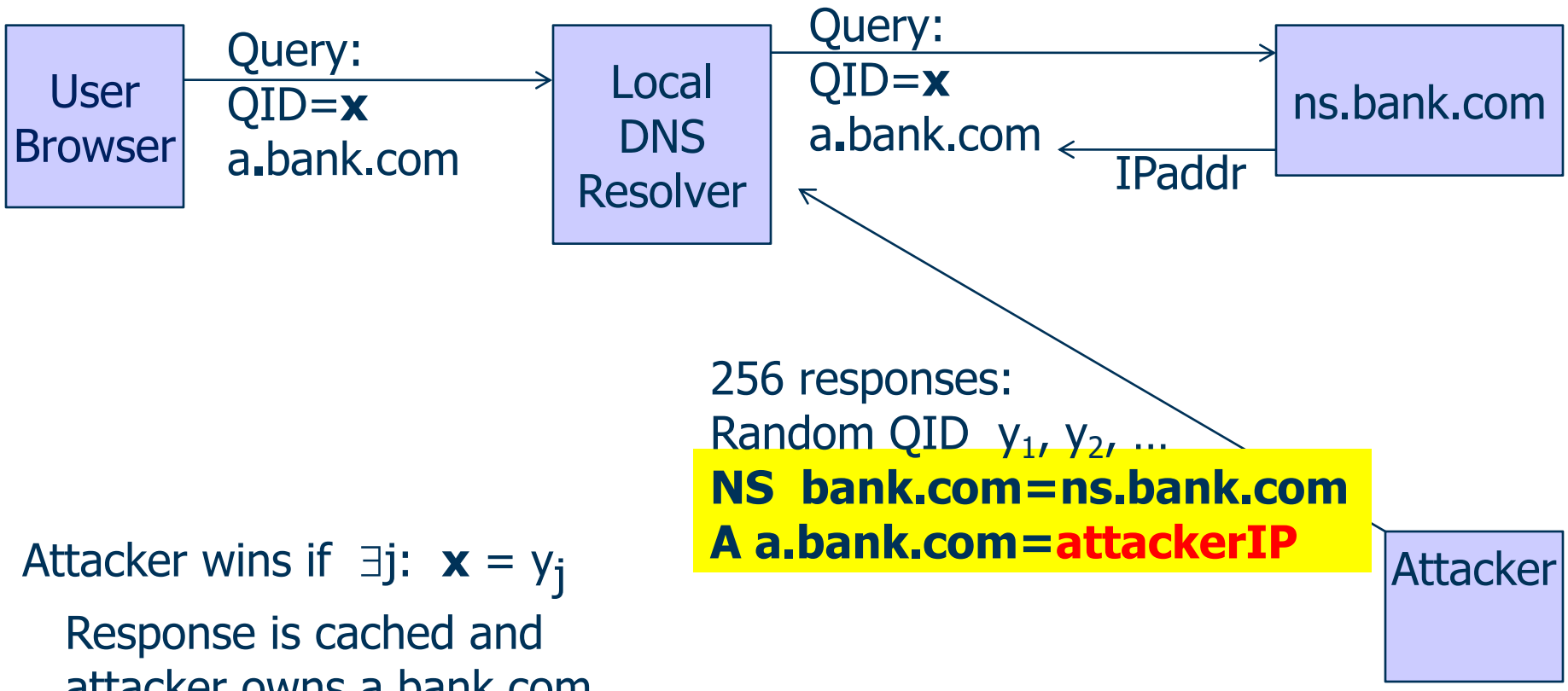
DNS CACHING

- Caching can substantially reduce overhead
  - The top-level servers very rarely change
  - Popular sites are visited often
  - Local DNS server often has the information cached
- How DNS caching works
  - DNS servers cache responses to queries
  - Response includes a TTL field
  - The server deletes the cached entry after TTL expires
- DNS negative queries are cached
  - Save time for non-existent sites, e.g., misspelling

DNS CACHE POISIONING ATTACK

- Basic idea: Give DNS servers a false record and get it cached
- Cache may be poisoned when a name server:
  - Disregards identifiers
  - Has predictable ID in query
  - Accepts unsolicited DNS records
- Some DNS server implementations do not validate the authority of a responder!

DNS CACHE POISIONING ATTACK



Attacker wins if $\exists j$: **x** = y_j

Response is cached and attacker owns a.bank.com

Success after ≈ 256 tries

DNS CACHE POISIONING PREVENTION

- Always check identifiers
- Make it hard to guess identifiers for queries (QID)
  - Use random QID
  - Increase size of QID
- Port randomisation for DNS requests
- Ask DNS query twice
- Deploy DNSSEC

SOME TOOLS

- dig
- host
- nslookup
- whois

SUMMARY

- DNS provides a hierarchical name space
- DNS is vulnerable to cache poisoning

RESOURCES

- **DNS.**
  Available at: https://www.ietf.org/rfc/rfc1034.txt
  Available at: https://www.ietf.org/rfc/rfc1035.txt

Questions?

Thanks for your attention!