The Domain Name System Security (DNSSEC)

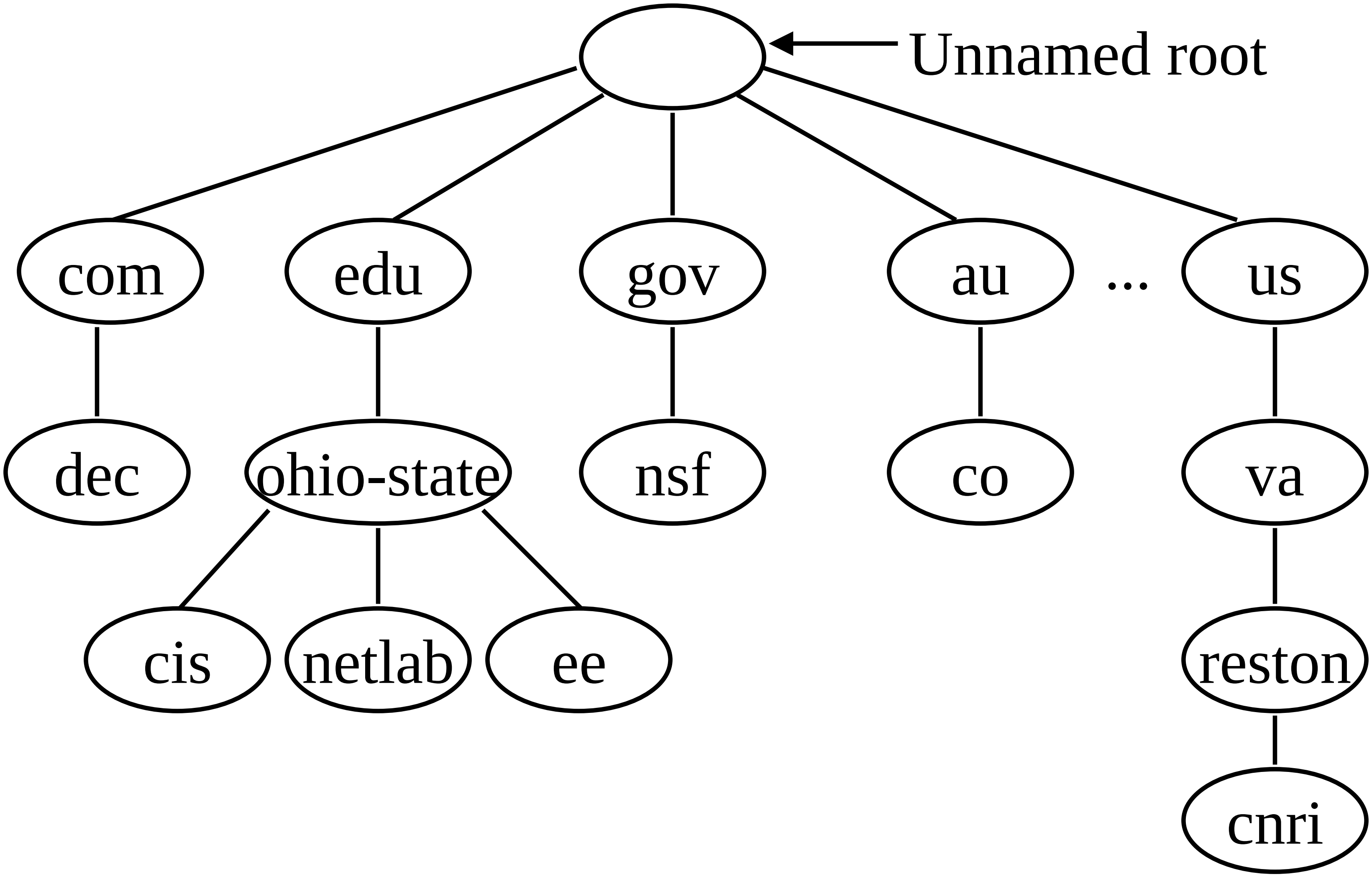
Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

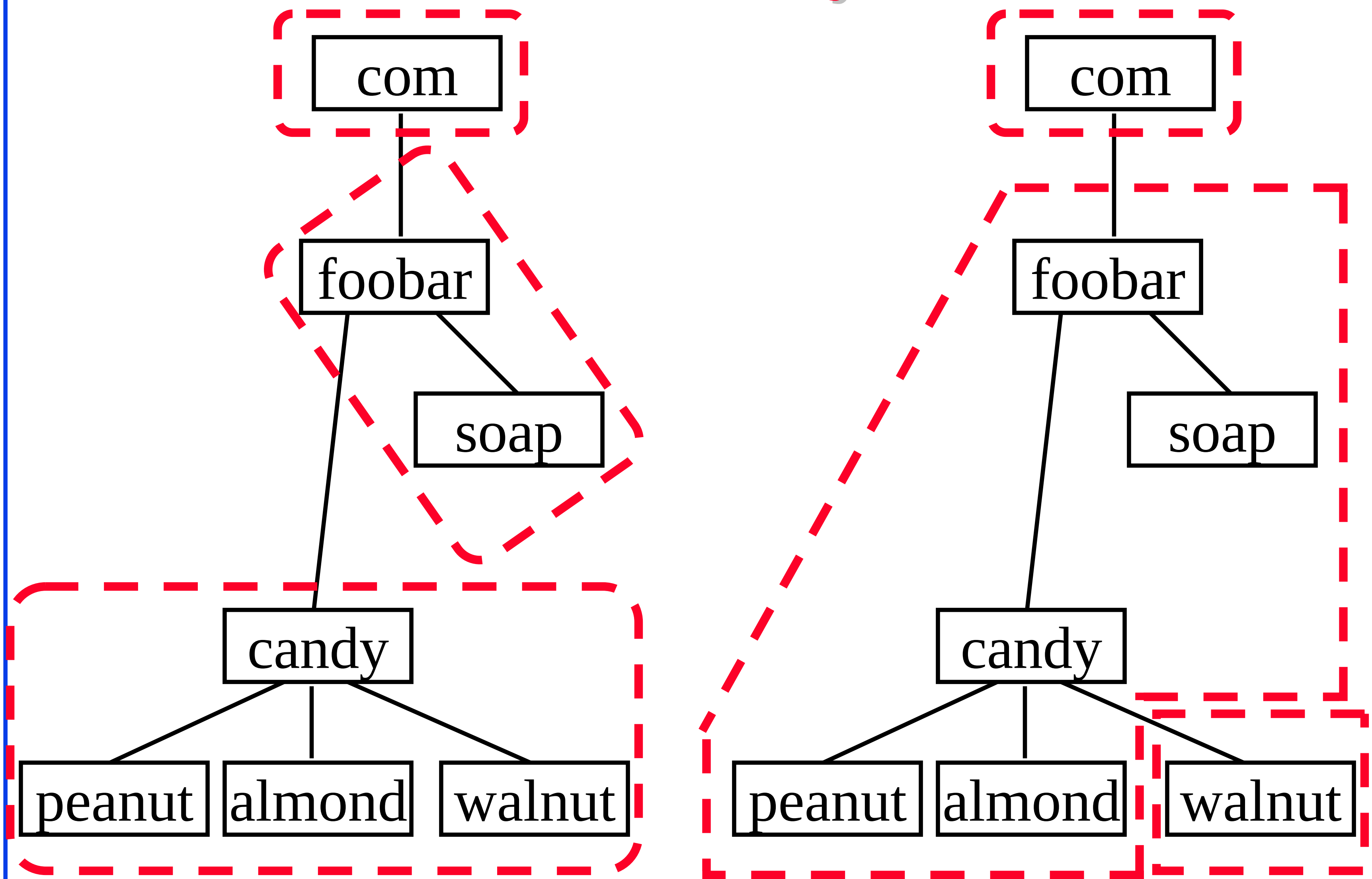
http://www.cse.wustl.edu/~jain/cse571-07/

- Naming hierarchy
- Server hierarchy
- Name resolution
- DNS Attacks
- DNS Security Mechanisms

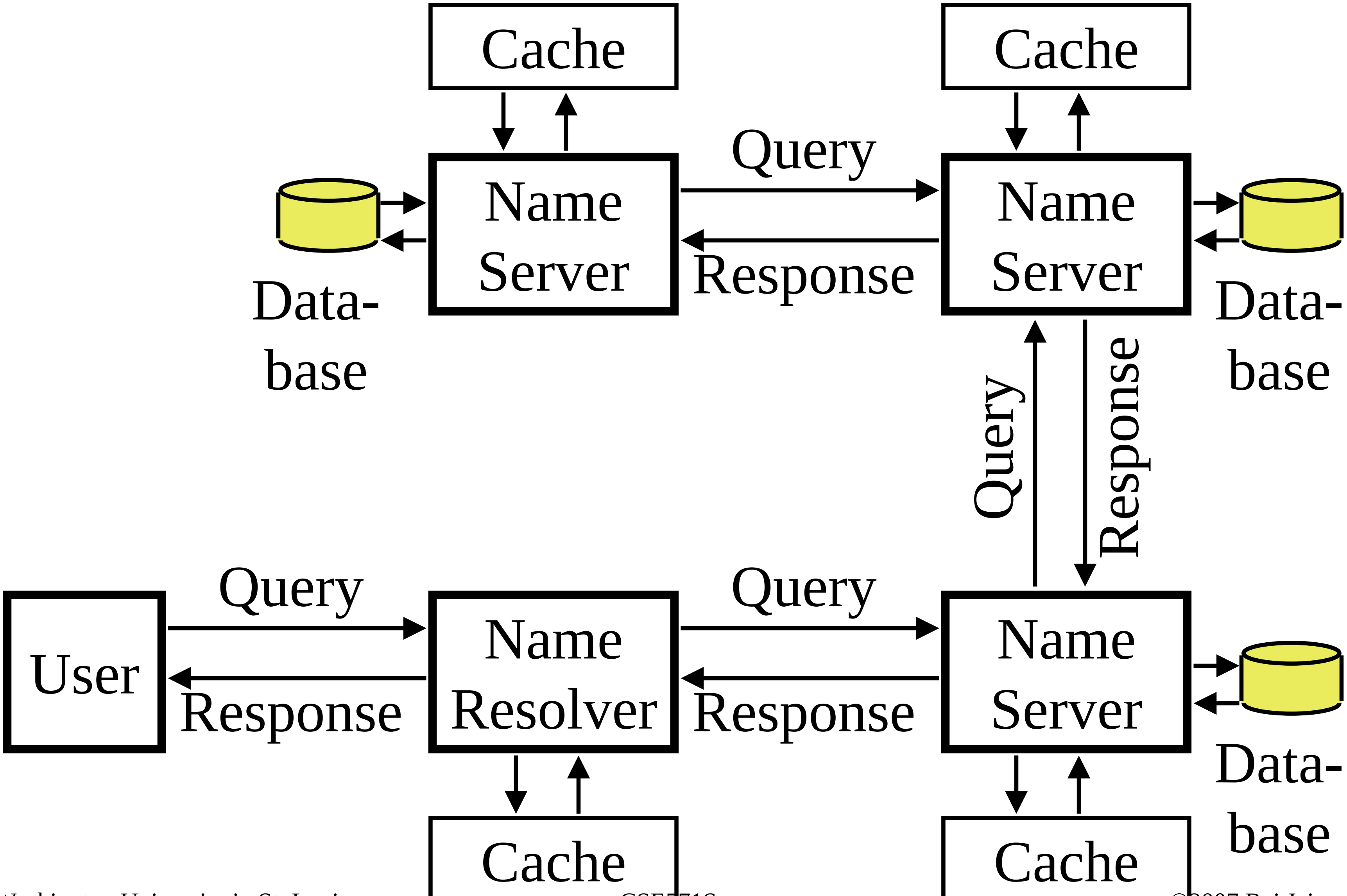
Name Hierarchy



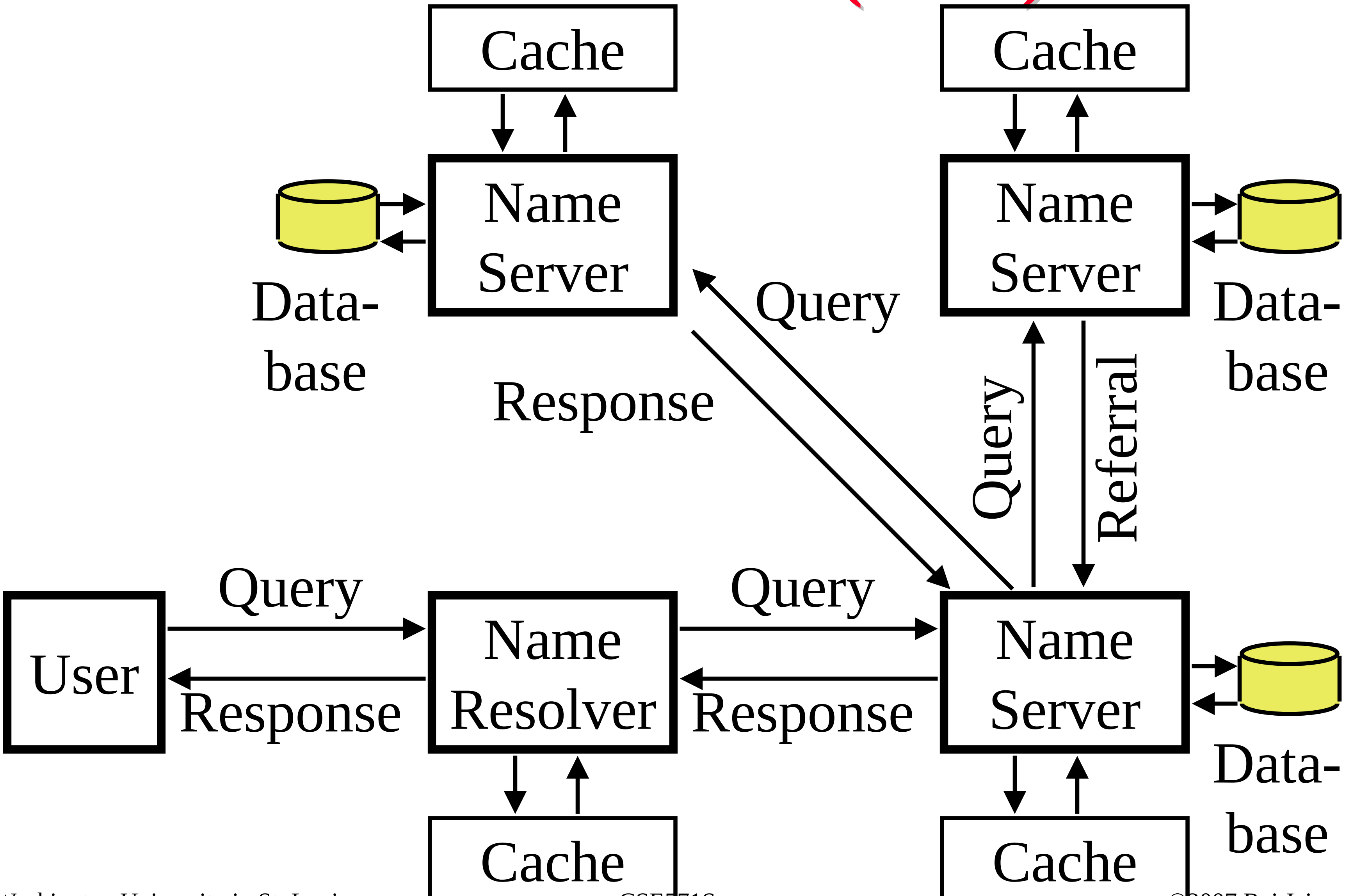
Server Hierarchy: Zones



Name Resolution



Name Resolution (Cont)



Name Resolution (Cont)

- Each computer has a name resolver routine, e.g., gethostbyname in UNIX
- Each resolver knows the name of a local DNS server
- Resolver sends a DNS request to the server
- DNS server either gives the answer, forwards the request to another server, or gives a referral
- Referral = Next server to whom request should be sent

Name Resolution (Cont)

- Resolvers use UDP (single name) or TCP (whole group of names)
- Knowing the address of the root server is sufficient
- Recursive Query:
  Give me an answer (Don't give me a referral)
- Iterative Query:
  Give me an answer or a referral to the next server
- Resolvers use recursive query.
- Servers use iterative query.

DNS Optimization

- Spatial Locality: Local computers referenced more often than remote
- Temporal Locality: Same set of domains referenced repeatedly $\Rightarrow$ Caching
- Each entry has a time to live (TTL)
- Replication: Multiple servers. Multiple roots. Ask the geographically closest server.

Types of DNS Entries: Resource Records

- DNS is used not just for name to address resolution
- But also for finding mail server, pop server, responsible person, etc for a computer
- DNS database has multiple types
- Record type A $\Rightarrow$ Address of X
- Record type MX $\Rightarrow$ Mail exchanger of X
- CNAME entry = Alias name (like a file link), "see name"
- www.foobar.com = hobbes.foobar.com

Resource Record Types

Type	Meaning
A	Host Address
CNAME	Canonical Name (alias)
HINFO	CPU and O/S
MINFO	Mailbox Info
MX	Mail Exchanger
NS	Authoritative name server for a domain
PTR	Pointer to a domain name (link)
RP	Responsible person
SOA	Start of zone authority (Which part of naming hierarchy implemented)
TXT	Arbitrary Text

Zone Transfer

- A zone should have more than one name server
- Secondary servers can acquire updates from primary server using zone transfer protocol
- DNS Dynamic Update
  - Ask primary server to add or delete DNS entries

Domain Name Systems Attacks

1. Cache Poisoning Attack
2. DNS Denial of Service Attack
3. DNS Dynamic Update Attack
4. Enumeration Attack
5. Non-rooted Non-FQDNs Problem

Cache Poisoning Attack

- A name server passes incorrect information to another name server ⇒ Victims are asked to go to incorrect sites
- One way is to send a query for a DNS zone for which attacker's server is authoritative
- Query: x.ibm.com IN A (What's address of x.ibm.com?)
- Answer: No response (I Don't know)
- Authority: wustl.edu. 3600 IN NS ns.attacker.com
  (the name server for wustl.edu is ns.attacker.com)
- Additional Section: ns.attacker.com IN A 128.245.23.45
  (The address for ns.attacker.com is 128.245.23.45)
- All queries for wustl.edu domain will now be directed to 128.245.23.45

Cache Poisoning Attack (Cont)

- Used by Kashpureff to redirect InterNIC to his AlterNIC (To protest InterNIC's control over DNS)
- Protection: Use inverse address query
  - 45.23.245.128.in-addr.arpa. ⇒ attacker.com

DNS Denial of Service Attack

1. Poison the cache and then return "not resolvable" for all addresses
   - Example: cse.wustl.edu is not resolvable authoritative answer
2. Return thousands of responses to every query
3. Add a CNAME record that points to itself
   - CNAME=Canonical Name $\Rightarrow$ Look up this alternate name
   - Infinite cycle

DNS Dynamic Update Attack

- Dynamic Host Control Protocol (DHCP) servers need to change DNS records
- Dynamic update protocol has been developed to allow such servers to add and delete DNS records
- Only certain systems can add or delete
- IP spoofing allows attackers use dynamic update protocol to change DNS records

Enumeration Attack

- Zone transfers are designed to allow secondary name servers to get incremental changes or complete database from primary server
- Attackers can use "Zone Transfer" to get entire DNS database
- Alternately use a DNS tool to query all IP addresses one-by-one
- System names often give out project information

Non-rooted Non-FQDNs Problem

- Described in RFC 1535, October 1993
- Fully qualified domain name (FQDN): cse.wustl.edu. (rooted)
- Non-rooted names resolved by trying many possibilities:
  - If jain@arl.cse.wustl.edu trys to reach www.ese
  - Resolver will try:
    - www.ese.cse.wustl.edu
    - www.ese.wustl.edu
  - If jain@arl.cse.wustl.edu trys to reach www.ibm.com
    - www.ibm.com.cse.wustl.edu.
    - www.ibm.com.wustl.edu.
    - www.ibm.com.edu.
    - www.ibm.com.
- If someone registers com.edu, they will get all such references.

Non-rooted Non-FQDNs Problem (Cont)

Solution: Divide the domain name into publicly and locally administered part

- jain@cse is local, wustl.edu is publicly administered
- Name resolver should try all combinations only within the locally administered part
- If jain@arl.cse.wustl.edu trys to reach www.ibm.com
- Resolver will try:
  - www.ibm.com.cse.wustl.edu.
  - www.ibm.com.wustl.edu.
  - www.ibm.com.

DNS Security Extensions

- RFC 4033, RFC 4034, RFC 4035, March 2005

A. 4 DNSSEC Resource Records

- DNS Public Key (DNSKEY)
- Resource Record Signature (RRSIG): secret key or public key
- Delegation Signer (DS)
- Next Secure (NSEC)

B. Two header flags:

- Checking Disabled (CD) in requests
  ⇒ I know how to verify signatures. Don't check for me.
- Authenticated Data (AD) in responses ⇒ I checked it out

C. Extensibility mechanism to allow large messages (EDNS0)

D. DNSSEC OK (DO) bit in EDNS header
  ⇒ I want secure answers

DNSKEY Resource Records

- Provides public key for any name
- Resolvers use the key to validate the signatures
- Includes key, algorithm type, protocol type, and flags
- Algorithms: RSA/MD5, Diffie-Hellman, Digital Signature Algorithm (DSA)
- Protocols = TLS, Email, DNSSEC, IPsec, ...
- Flag bits indicate key usage: authentication, confidentiality, ...

Secret Key Transaction Authentication

- RFC 2845, May 2000
- Transaction signatures (TSIG) RR using pair-wise secrets
- Authenticate Dynamic Updates and Resolution responses
- Good for authenticating clients or resolvers to local servers
- Not good for server-to-server authentication (use Public Key)
- HMAC-MD5 or HMAC-SHA1 is used
- Requests contain TSIG
- Responses contain TSIG on the concatenation of request and response ⇒ Transactions and request authentication
- In both cases time value is included
- Forwarding resolvers pass TSIG (if no shared secret) or replace TSIG (if shared secret)
- TSIGs are not cached or stored

Public Key Transaction Authentication

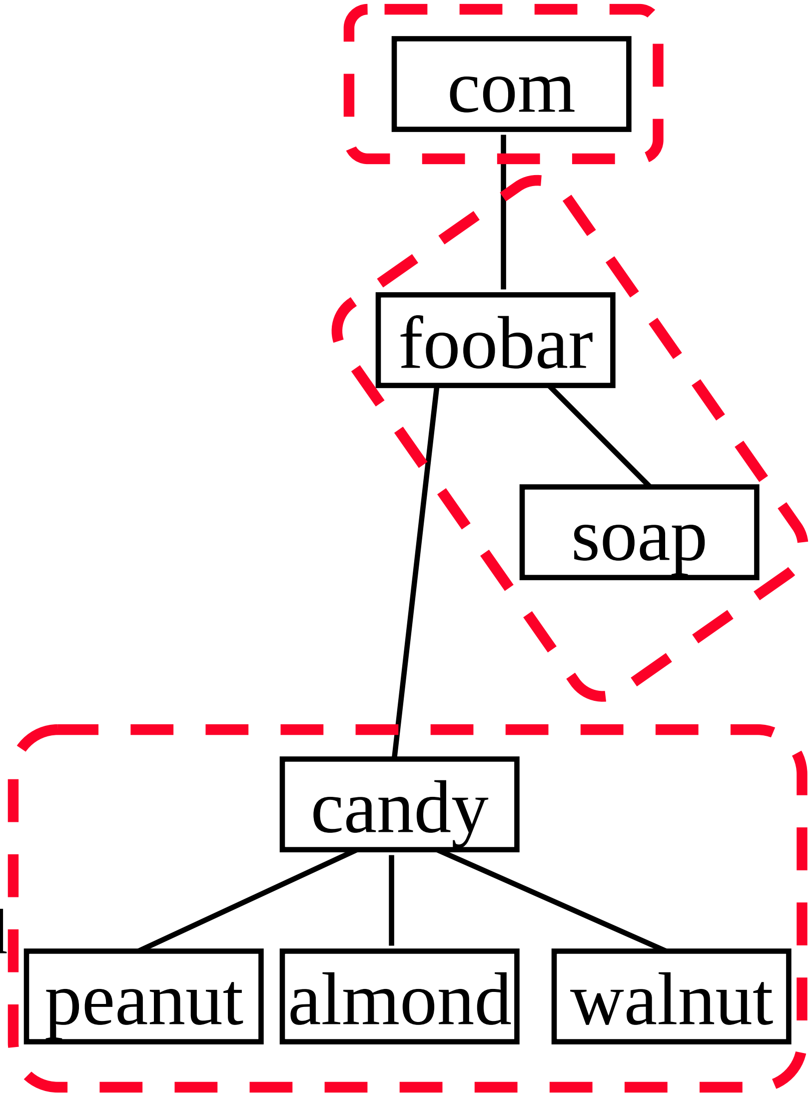
- RFC 2931, Sep 2000
- SIG(0)s resource records using public key method
- Get the signed public key of the server and validate it
- Send a request with SIG(0) = MAC based on public key
- Get a response with SIG(0) = MAC on the response and request based on private key
- More expensive than TSIG
- SIG(0) on requests are optional
- SIG(0) on responses are generated when requested

DNSSEC Keys

- Key signing key: To sign DNSKEY RRs
- Zone key: To sign other RRs for the zone
- Although not required, it is better to keep the two keys separate.
- Key signing key can be much longer, much less used
  $\Rightarrow$ Changed infrequently (13 months)
  - Private key can be kept offline
- Zone key can be shorter, frequently changed (1 month)
  - Private Zone key may be required to kept on-line (vulnerable)

Delegation Signer Resource Record

- DS RR, RFC 3658, Dec 2001
- The DNS key must be signed by the parent
- Issue: Every time child changes key, parent must sign
- Better: Parent signs the key child uses to sign its key (key signing key)
- Child apex can change the key frequently and have multiple keys for multiple protocols
- DS RR at parents are used to find key signing key for the child zone



Next (NXT) RR

- DNS allows negative response, e.g., X.wustl.edu does not exist
- All names in the zone are sorted (in canonical order) and the next name is returned in the negative response
  - x.wustl.edu does not exist, the next name is x1.wustl.edu
- This can be signed using SIG RR

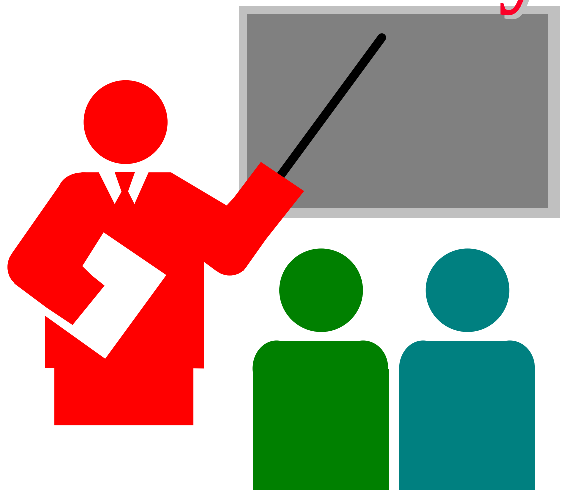
Extensibility Mechanism (EDNS0)

- RFC 2671, August 1999
- RFC 3226, December 2001
- A previously reserved field is used for extension flags
- DNSSEC OK = DO bit
  $\Rightarrow$ Client understands DNSSEC
- Another option indicates UDP payload size > 512B
- DNSSEC clients should use between 1220 to 4000B messages

DNSSEC Features

- Provides:
  - Origin Authentication
  - Integrity
  - Public Key Distribution
  - Authenticated denial of existence
- Does not provide:
  - Confidentiality (Use IPsec)
- Protects against cache poisoning
- Does not protect against DoS
- **Status**: .se is the first domain to try DNSSEC

Summary



- DNS: Maps names to addresses
- Names are hierarchical. Administration is also hierarchical.
- DNSSEC provides authentication of data, data source and has mechanisms to distributed public keys
- Performance hit $\Rightarrow$ Not yet widely deployed

DNSSEC RFCs

- RFC 1535 "A Security Problem and Proposed Correction With Widely Deployed DNS Software," October 1993.
- RFC 2845 "Secret Key Transaction Authentication for DNS (TSIG)," May 2000.
- RFC 3007 "Secure DNS Dynamic Update," November 2000.
- RFC 3130 "Notes from the State-Of-The-Technology: DNSSEC," June 2001.
- RFC 3225 "Indicating Resolver Support of DNSSEC," December 2001.
- RFC 3226 "DNSSEC and IPv6 A6 aware server/resolver message size requirements," December 2001.
- **RFC 4033 "DNS Security Introduction and Requirements," March 2005.**

DNSSEC RFCs (Cont)

- RFC 4034 "Resource Records for the DNS Security Extensions," March 2005.
- RFC 4035 "Protocol Modifications for the DNS Security Extensions," March 2005.
- RFC 4310 "DNS Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)," December 2005.
- RFC 4431 "The DNSSEC Lookaside Validation (DLV) DNS Resource Record," February 2006.
- RFC 4470 "Minimally Covering NSEC Records and DNSSEC On-line Signing," April 2006.
- RFC 4509 "Use of SHA-256 in DNSSEC Delegation Signer (DS) RRs," May 2006.
- RFC 4641 "DNSSEC Operational Practices," September 2006.
- RFC 4955 "DNSSEC Experiments," July 2007.

DNSSEC RFCs (Cont)

- RFC 4956 "DNSSEC Opt-In," July 2007.
- RFC 4986 "Requirements Related to DNSSEC Trust Anchor Rollover," August 2007.
- RFC 5011 "Automated Updates of DNSSEC Trust Anchors," September 2007.

Other References

- DNS Security, http://compsec101.antibozo.net/papers/dnssec/dnssec.html
- _DNSSEC: DNS Security Extensions, http://www.dnssec.net/
- DNS Cache Poisoning, http://en.wikipedia.org/wiki/DNS_cache_poisoning