

Übung Verteilte Systeme / Ubiquitous Computing

Übungsblatt 3

30. November 2007

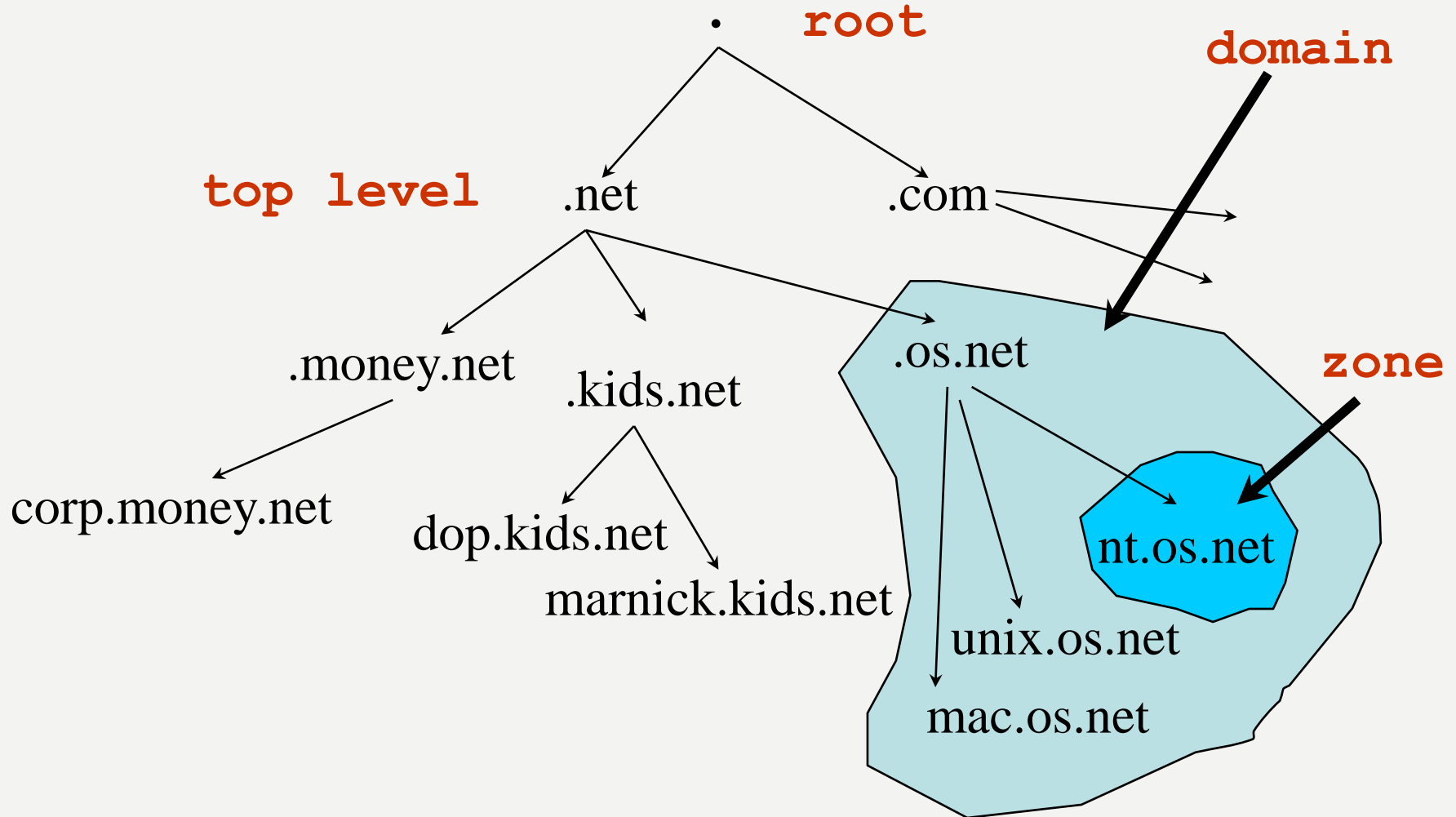


Aufgabe 10: DNSSEC



- Overview of DNS
- Motivation
- PK-DNSSEC
- SK-DNSSEC
- Comparison with PK-DNSSEC
- Usage of DNSSEC

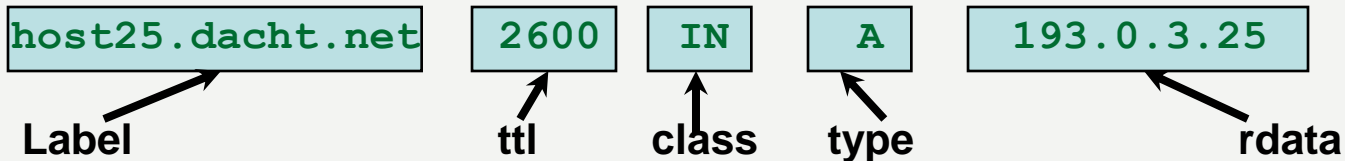
- Domain Name System
- Distributed ‘database’ to resolve domain names
- Labels translate to Resource Records
 - Address (A)
 - Mail hosts (MX)
 - Text (TXT)
 - and much more....
- Resource records stored in zones
- Highly scalable



Example Zone file

```
dacht.net 7200 IN SOA ns.ripe.net. olaf.ripe.net. (  
    2001061501 ; Serial  
    43200 ; Refresh 12 hours  
    14400 ; Retry 4 hours  
    345600 ; Expire 4 days  
    7200 ; Negative cache 2 hours  
)
```

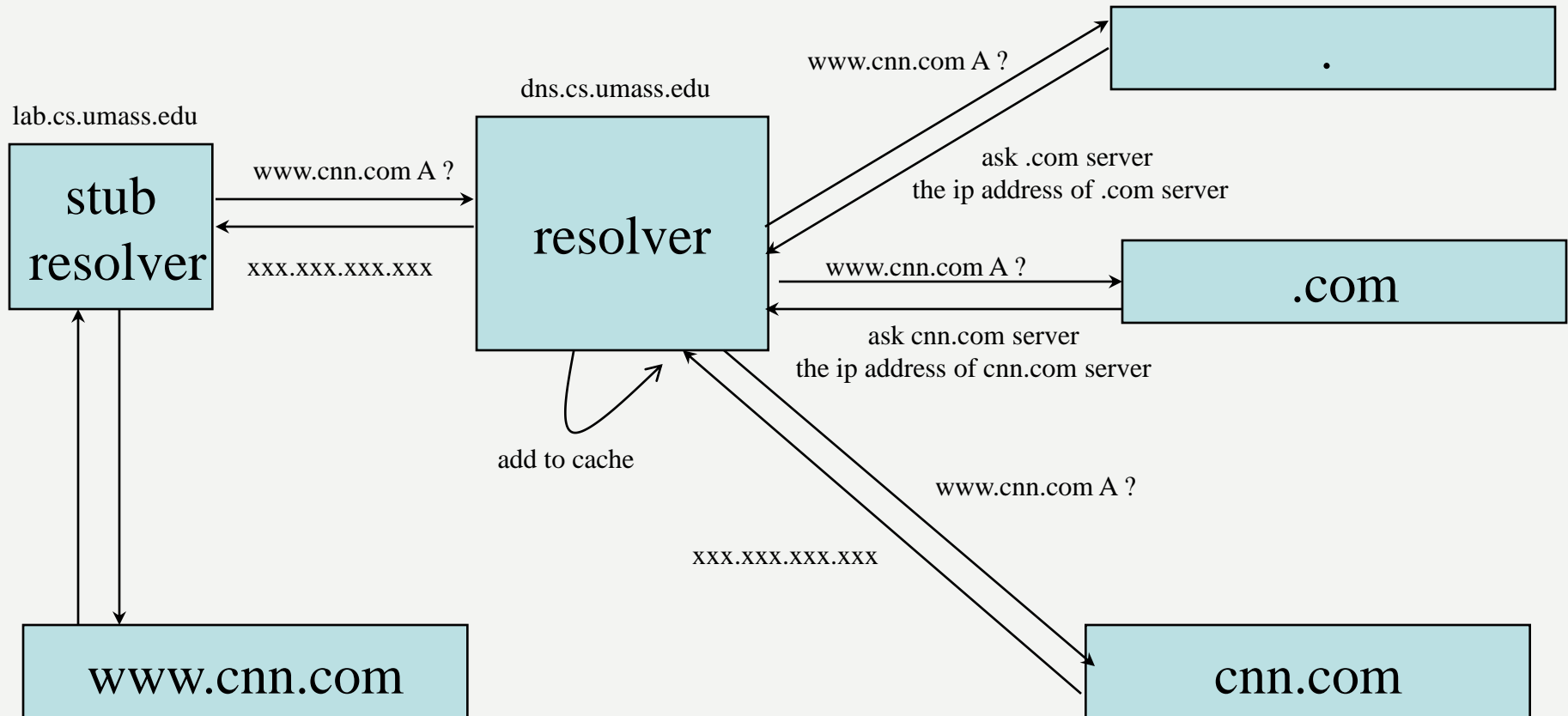
```
dacht.net 7200 IN NS ns.ripe.net.  
dacht.net 7200 IN NS ns.high5.net.  
pinkje.dacht.net 3600 IN A 193.0.1.162  
host25.dacht.net 2600 IN A 193.0.3.25
```



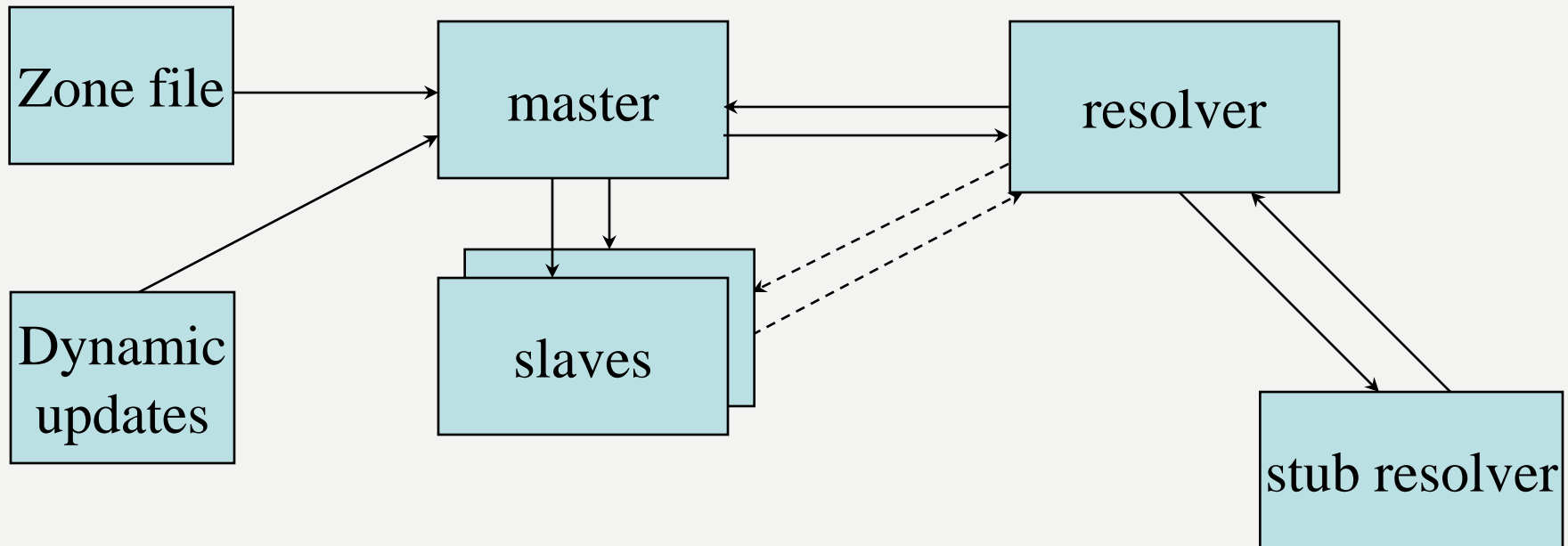
Label ttl class type rdata

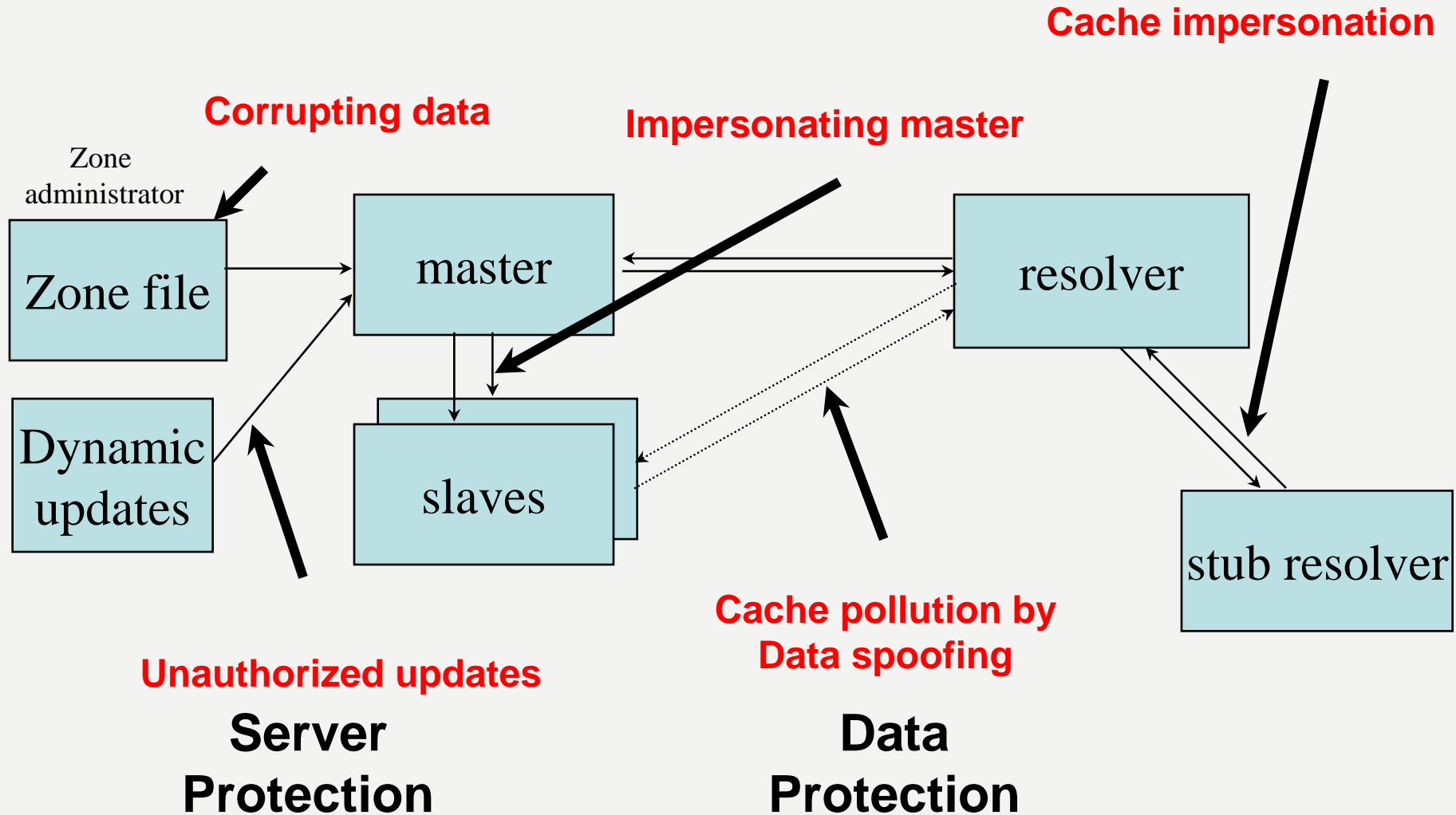
RECORD TYPE	DESCRIPTION	USAGE
A	An address record	Maps FQDN into an IP address
PTR	A pointer record	Maps an IP address into FQDN
NS	A name server record	Denotes a name server for a zone
SOA	A Start of Authority record	Specifies many attributes concerning the zone, such as the name of the domain (forward or inverse), administrative contact, the serial number of the zone, refresh interval, retry interval, etc.
CNAME	A canonical name record	Defines an alias name and maps it to the absolute (canonical) name
MX	A Mail Exchanger record	Used to redirect email for a given domain or host to another host

Question: www.cnn.com



Zone administrator



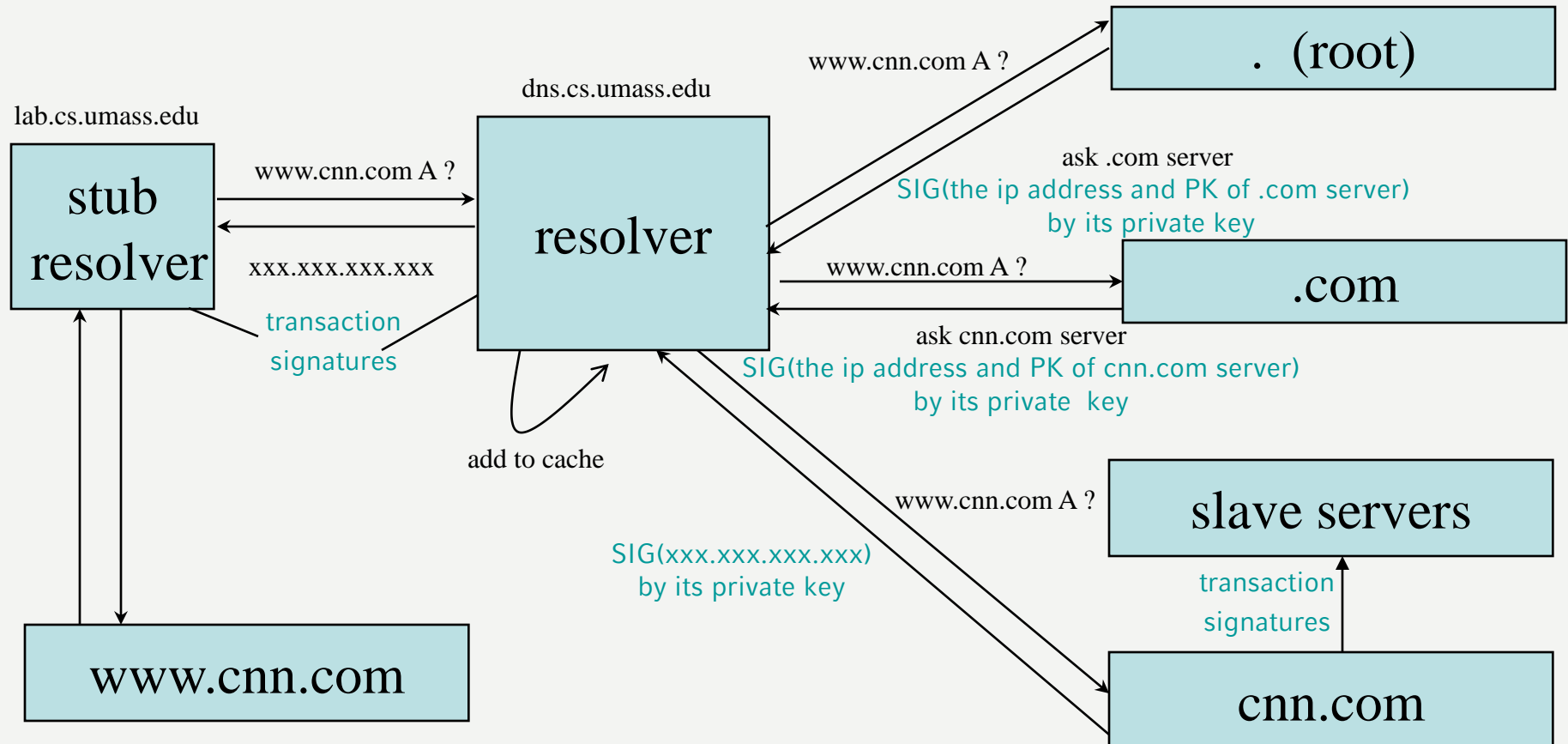


- DNSSEC protects against data spoofing and corruption
- DNSSEC also provides mechanisms to authenticate servers and requests
- DNSSEC provides mechanisms to establish authenticity and integrity

- The DNS servers sign (digitally encrypt) the hash of resource record set with its private keys
- Resource record set: The set of resource records of the same type.
- Public KEYs can be used to verify the SIGs
- The authenticity of public KEYs is established by a SIGnature over the keys with the parent's private key
- In the ideal case, only one public KEY needs to be distributed off-band (the root's public KEY)

- Cover each resource record set with a public-key signature which is stored as a resource record called SIG RR
- SIG RRs are computed for every RRset in a zone file and stored
- Add the corresponding pre-calculated signature for each RRset in answers to queries
- Must include the entire RRset in an answer, otherwise the resolver could not verify the signature

Question: www.cnn.com



- Global real time availability
 - Easy access to DNS
- Scalability
 - Hierarchical organization
- Globally unique names
 - Globally unique host name
- Cryptographic binding of name and key
 - KEY RR binds DNS names with keys

- Denial-of-Service-Attacken durch DNSSEC nicht verhindert
- sondern auf Grund des höheren Rechenaufwands auf den Servern sogar erleichtert.
- Verteilung der Schlüssel zur Bildung von Chains of Trust erfolgt manuell