7. DNS/DNSSEC and DANE

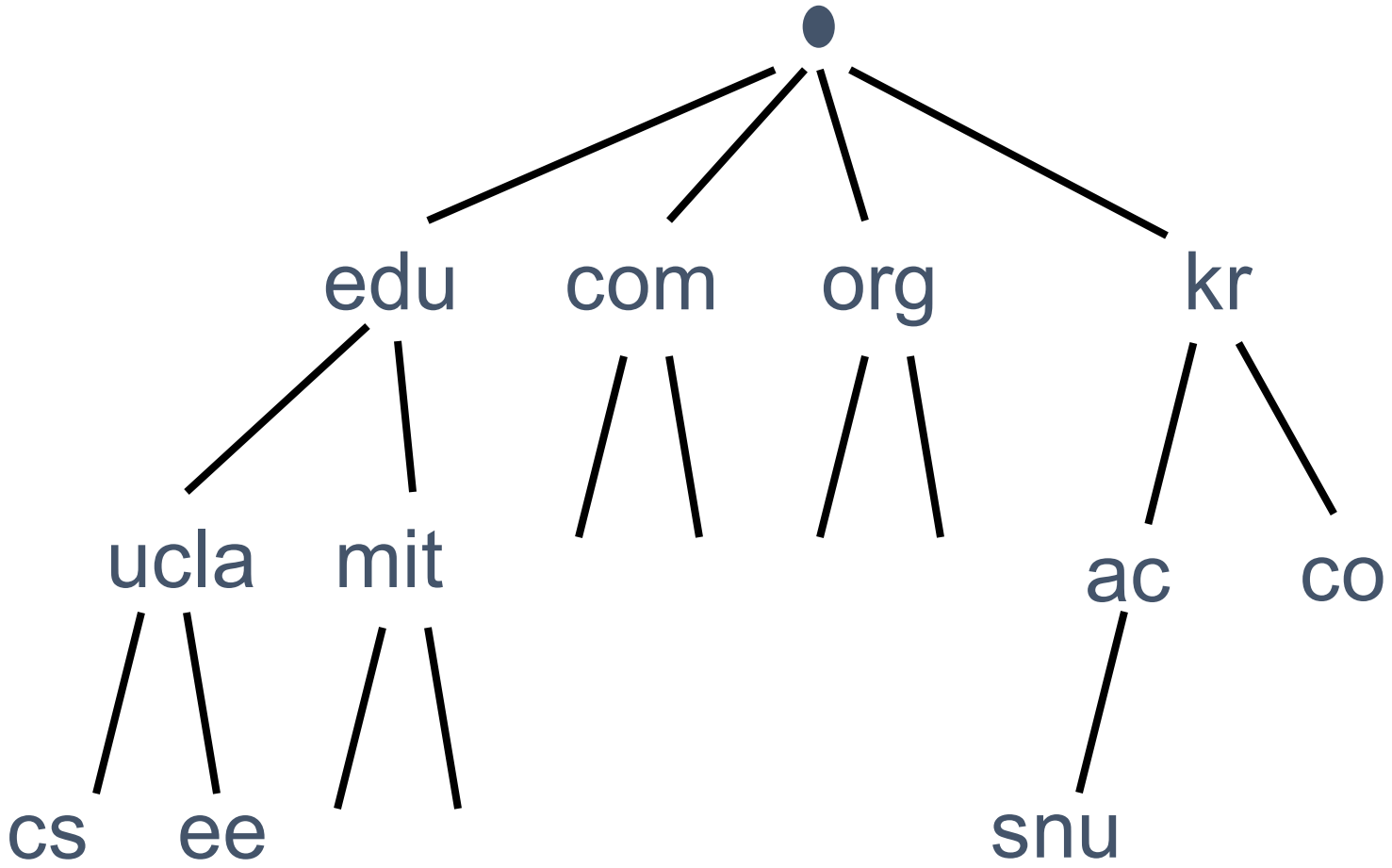
DNS/DNSSEC

DNS

- domain name system

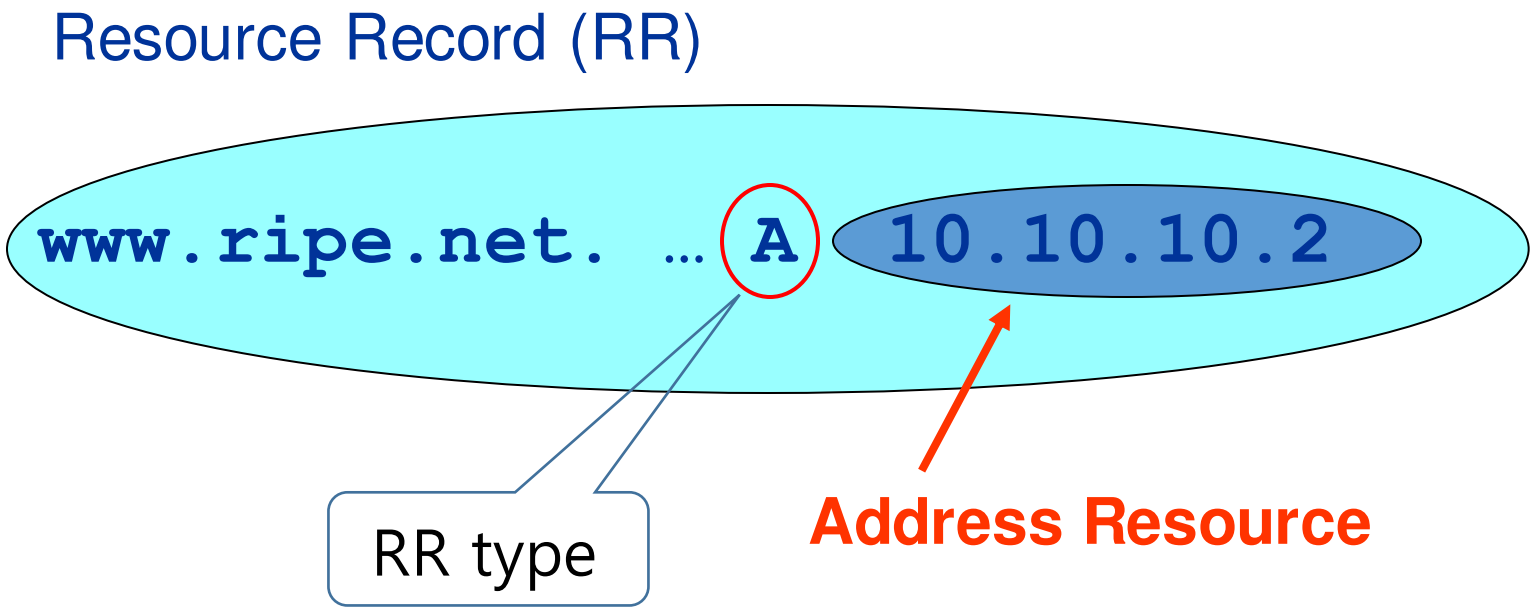
- provides IP address for a domain name
- a distributed DB

DNS Hierarchy



Concept: Resource Records

- The DNS maps names into data using Resource Records.



DNS RRs

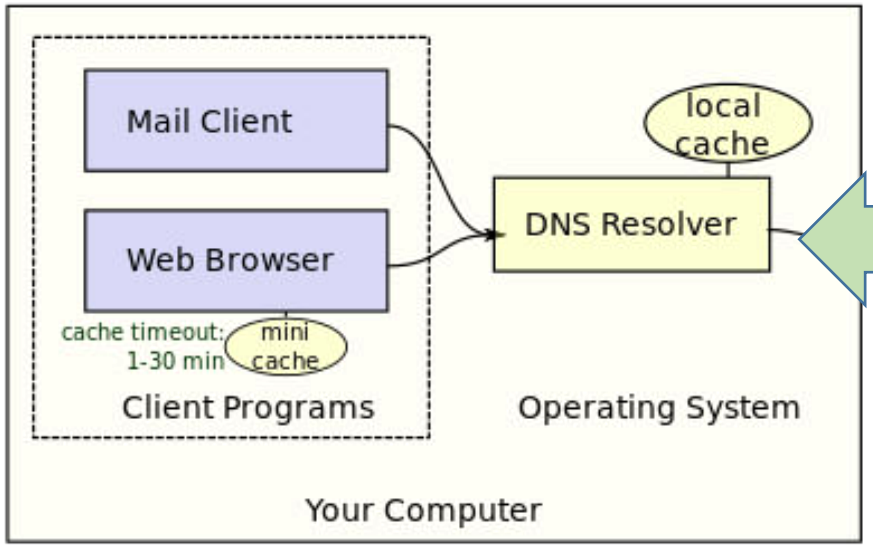
DNS: a distributed db storing resource records (RRs)

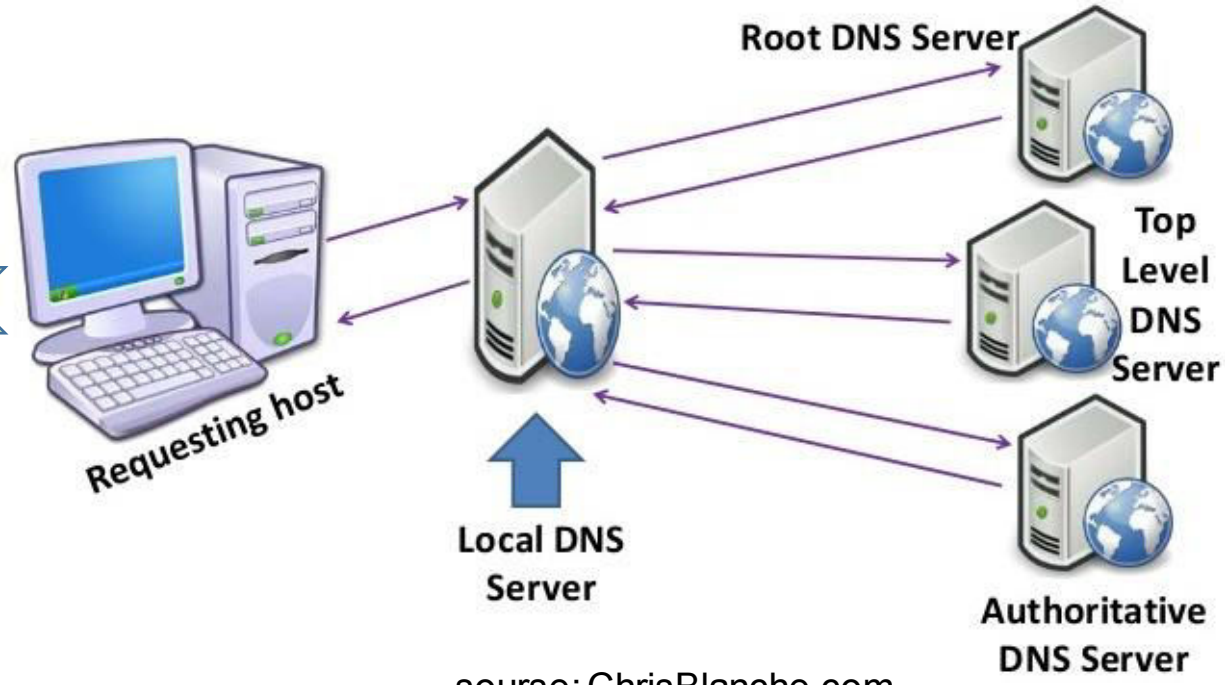
RR format: ***(name, ttl, class, type, value)***

- *Type=A*
  - ***name*** *is hostname*
  - ***value*** *is IP address*
  - *AAAA type for IPv6*
- *Type=NS*
  - ***name*** *is domain (eg., foo.com)*
  - ***value*** *is hostname of authoritative name server for this domain*
- *Type=CNAME*
  - ***name*** *is alias name for some "canonical" (the real) name, e.g., www.ibm.com is really servereast.backup2.ibm.com*
  - ***value*** *is canonical name*
- *Type=MX*
  - ***value*** *is name of mailserver associated with* ***name***

DNS: Stub Resolver vs local DNS server

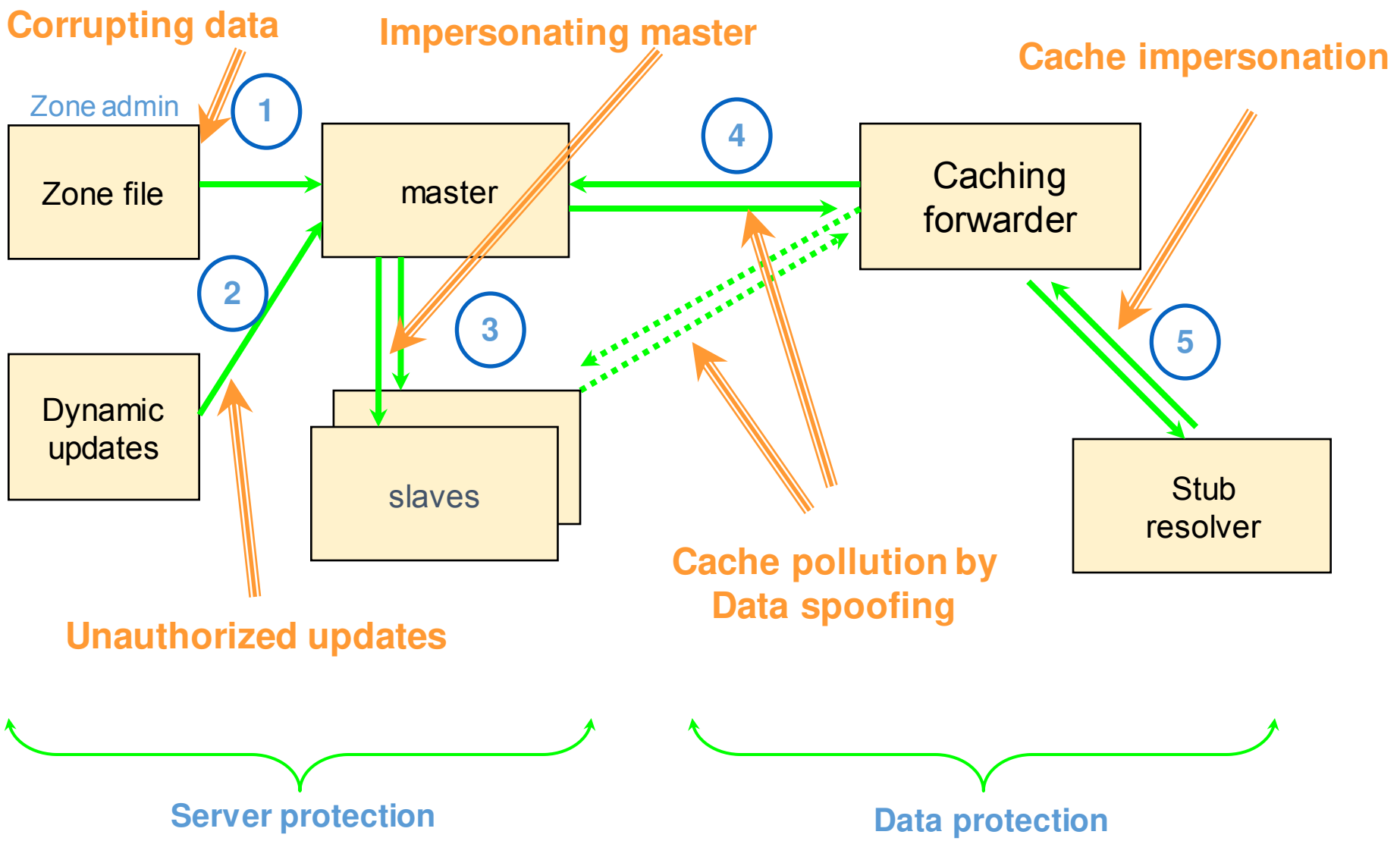
- Stub resolver
  - Not interact with the zone hierarchy
  - Pose basic queries to recursive servers
  - May cache answers
  - PC, client applications
- local DNS server
  - aka DNS forwarder
  - caches DNS response
  - performs domain name lookup on behalf of client
  - is usually located on the local network
  - If you use an ISP, your DNS server is at your ISP.





sourse: ChrisBlanche.com

DNS Vulnerabilities



Why DNSSEC: To protect the DNS itself

Current DNS suffers from DNS poisoning and domain hijacking attacks!!

DNSSEC protects against data spoofing and corruption

- DNSSEC also provides mechanisms to authenticate servers
- DNSSEC provides mechanisms to establish authenticity and integrity

- A secure DNS will be used as a PKI
  - However it is NOT a general purpose PKI

DNS RR Review

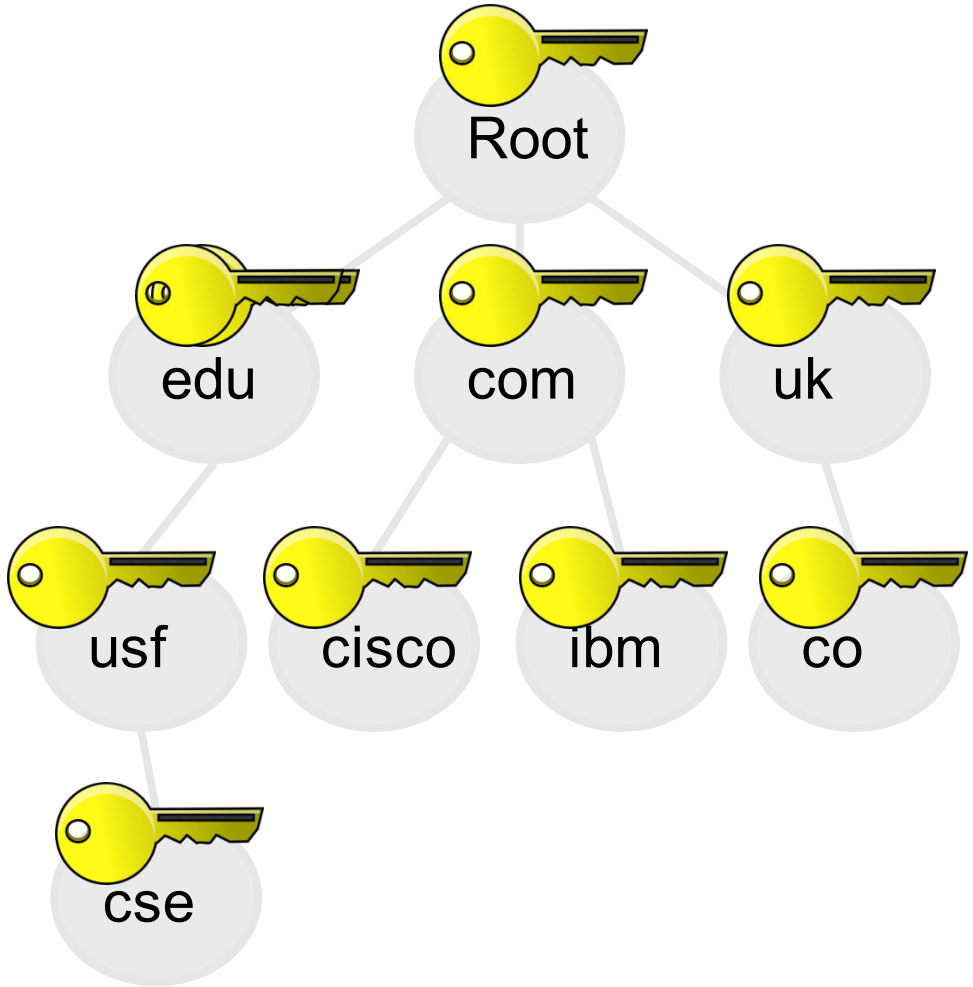
- DNS Resource Record (RR)
  - Can be viewed as tuples of the form
    <name, TTL, class, type, data>
  - types: A (IP address)
    MX (mail servers)
    NS (name servers)
    PTR (reverse look up)
    RRSIG (signature)
    DNSKEY (public key)
    DS (delegated signer)
    …
    TLSA (DANE)

Recap: RRs and RRsets

- Resource Record:
  - label class ttl type rdata
    www.ripe.net IN 7200 A 192.168.10.3
- All RRs of a given label, class, type make up an RRset:
    www.ripe.net IN 7200 A 192.168.10.3
    A 10.0.0.3
- In DNSSEC the RRsets are signed, not the individual RRs

DNSSEC

- Provides a “natural” PKI
  - Maps zones to their keys
  - Parent-zone sign child zones’ keys
- Keys organized as tree structure.
  - Each zone is the authority for its local data
  - A zone’s key is only effective for its zone

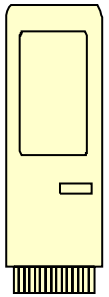


source: Prof. Xinming Ou@USF

Two key pairs for a zone

- Key Signing key (KSK)
  - a long term key
  - to compute a signature on the ZSK to allow it to be validated.
- Zone Signing Key (ZSK)
  - a short term key.
  - to routinely compute signatures for the DNS records
  - ZSK is changed or rolled over frequently
- KSK, in the form of a DS record that is passed up to the "parent" zone. The parent zone signs the DS record of the child with their own ZSK

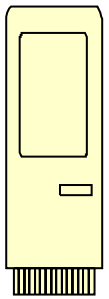
Key Management



NS for .edu

PK_{edu}

DS Record



NS for usf.edu

key signing key

PK_{usf}

PK_{usf2}

Want to change PK_{usf} to PK_{usf2}

sign

$Sig\{PK_{usf}\}_{PK_{edu}}$

$PK_{signing}$

Do not need to notify parent if changed

zone signing key

…

source: Prof. Xinming Ou@USF

DANE

RFC 6698

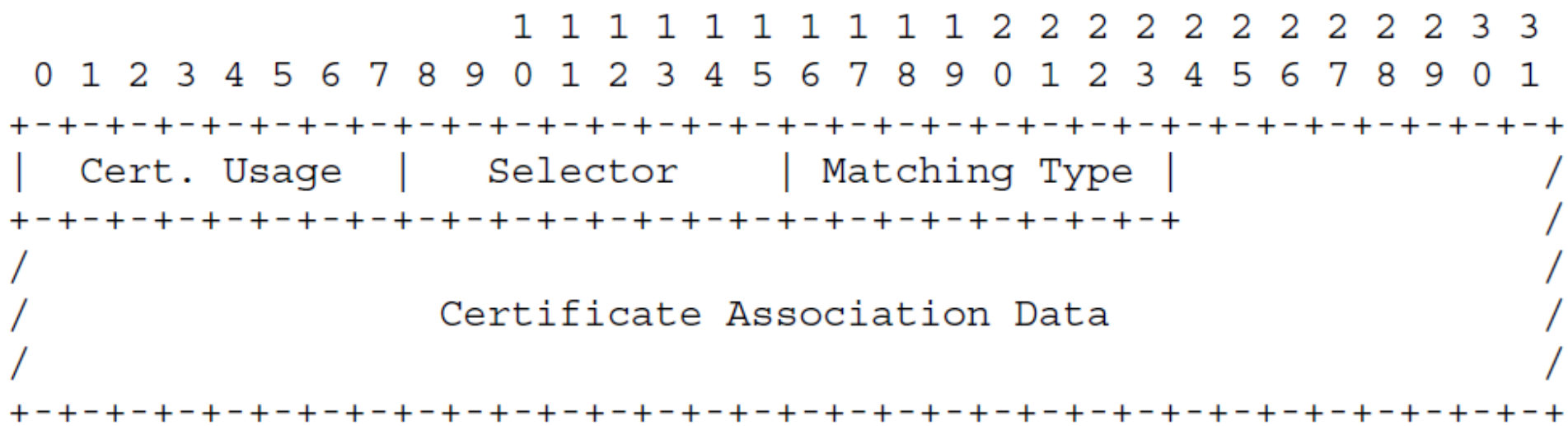
TLS and PKI

- TLS relies on server certificates
- CA security breach may issue a fraudulent certificate

- DANE allows domain owner to store keys/certificates used by TLS.
  - A new DNS record type: TLSA
  - must be DNSSEC signed
- DANE TLSA records only means that “this domain owner says…”

DANE: DNS-Based Authentication of Named Entities

- enables domain admin to specify/certify the CAs or public keys (or certs)
- RFC 6698, 7671
- TLSA parameters in resource record



TLSA RR parameters

- cert. usage
  - 0: CA cert. or its public key, called CA constraint
  - 1: end entity cert. or its public key, called service cert. constraint
  - 2: trust anchor cert. or its public key
  - 3: domain-issued cert. (not signed by CA)

Value	Acronym	Short Description	Reference
0	PKIX-TA	CA constraint	[RFC6698]
1	PKIX-EE	Service certificate constraint	[RFC6698]
2	DANE-TA	Trust anchor assertion	[RFC6698]
3	DANE-EE	Domain-issued certificate	[RFC6698]

TLSA RR parameters

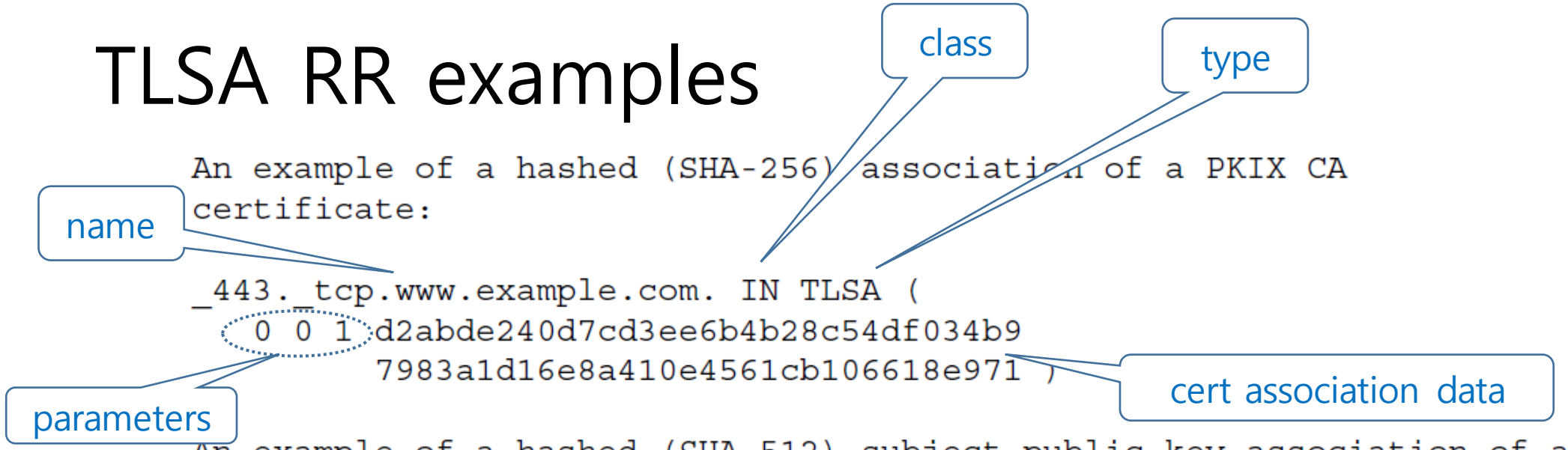
- selector: which part of cert will be matched against association data
  - 0: full cert
  - 1: SubjectPublicKeyInfo

Value	Acronym	Short Description	Reference
0	Cert	Full certificate	[RFC6698]
1	SPKI	SubjectPublicKeyInfo	[RFC6698]

TLSA RR parameters

- matching type
  - 0: exact match
  - 1: SHA-256 hash
  - 2: SHA-512
- cert. association data
  - raw data or its hash
  - of cert. or of its public key

TLSA RR examples

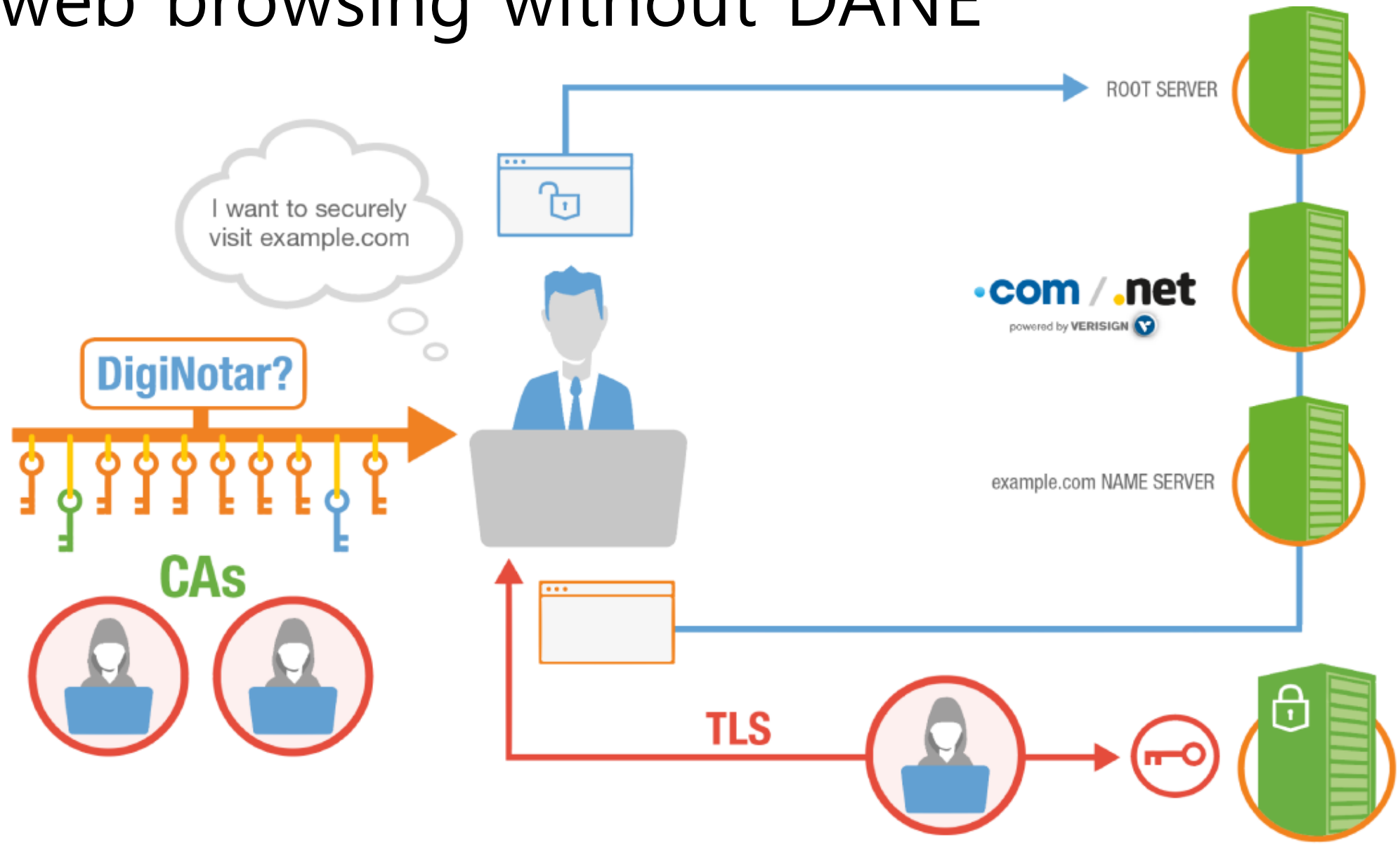



```
An example of a hashed (SHA-256) association of a PKIX CA
certificate:

_443._tcp.www.example.com. IN TLSA (
   0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
         7983a1d16e8a410e4561cb106618e971 )

An example of a hashed (SHA-512) subject public key association of a
PKIX end entity certificate:

_443._tcp.www.example.com. IN TLSA (
   1 1 2 92003ba34942dc74152e2f2c408d29ec
         a5a520e7f2e06bb944f4dca346baf63c
         1b177615d466f6c4b71c216a50292bd5
         8c9ebdd2f74e38fe51ffd48c43326cbc )

An example of a full certificate association of a PKIX end entity
certificate:

_443._tcp.www.example.com. IN TLSA (
   3 0 0 30820307308201efa003020102020... )
```

DANE configured browser

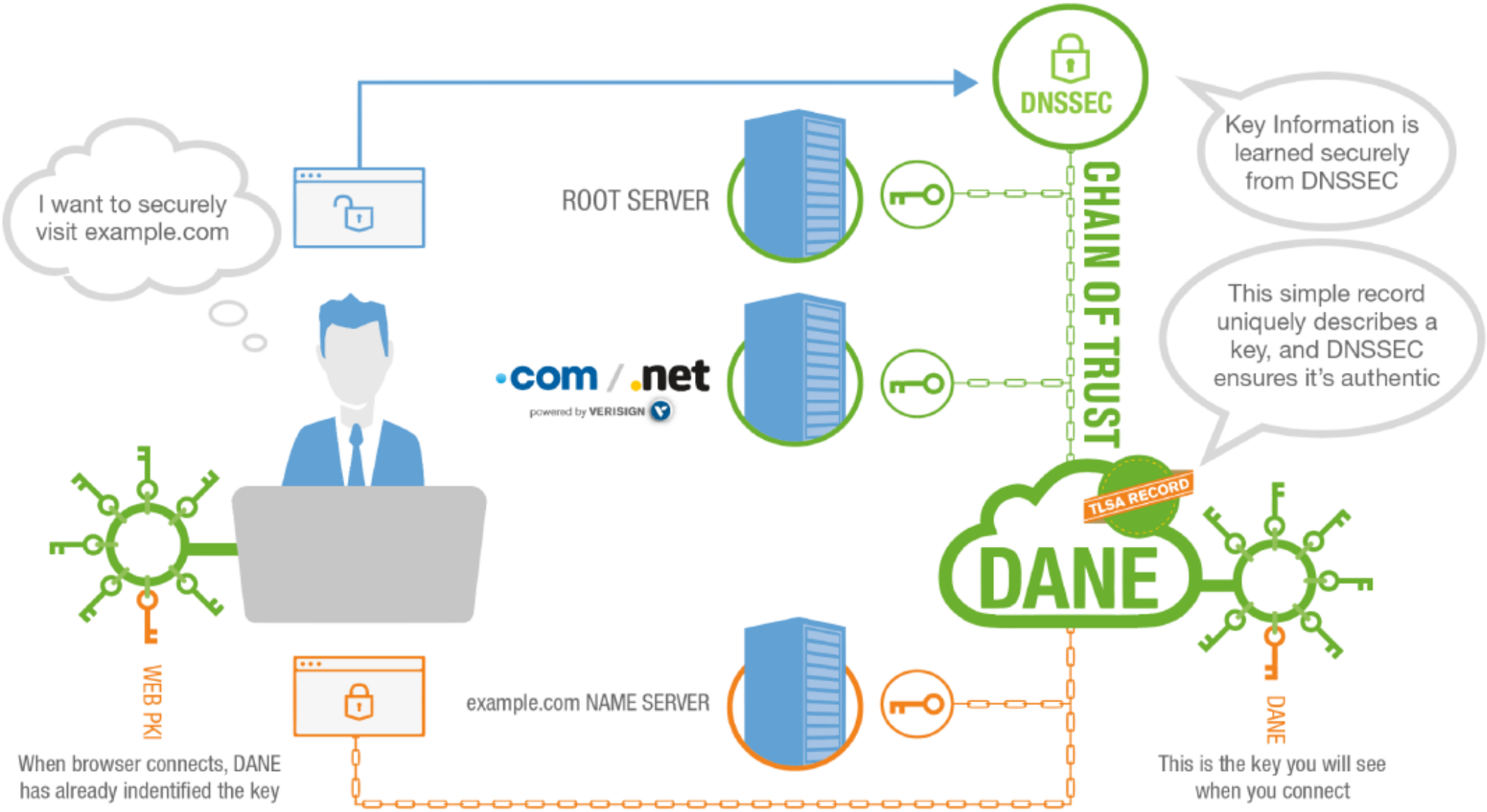
- browser queries for TLSA RRs for domain
- DNSSEC required
- compares the cert from TLS (website) and the one from DNS
- connection fails if mismatch

web browsing without DANE



source: VeriSign

web browsing with DANE



source: VeriSign

DANE: not just for web

- DANE defines how a user verifies the certificate of a domain from DNS
- other uses are possible
  - email (SMTP)
  - VoIP
  - Jabber/XMPP