CSE 127: Computer Security

Network Security

Kirill Levchenko

December 5, 2017

DNS

- **Domain Name System (DNS):** maps host names to addresses
  - Large distributed database
- Critical Internet infrastructure
  - Control of DNS allows attacker to impersonate any site (in the absence of end-to-end host authentication using SSH or TLS)
- Target of attacks

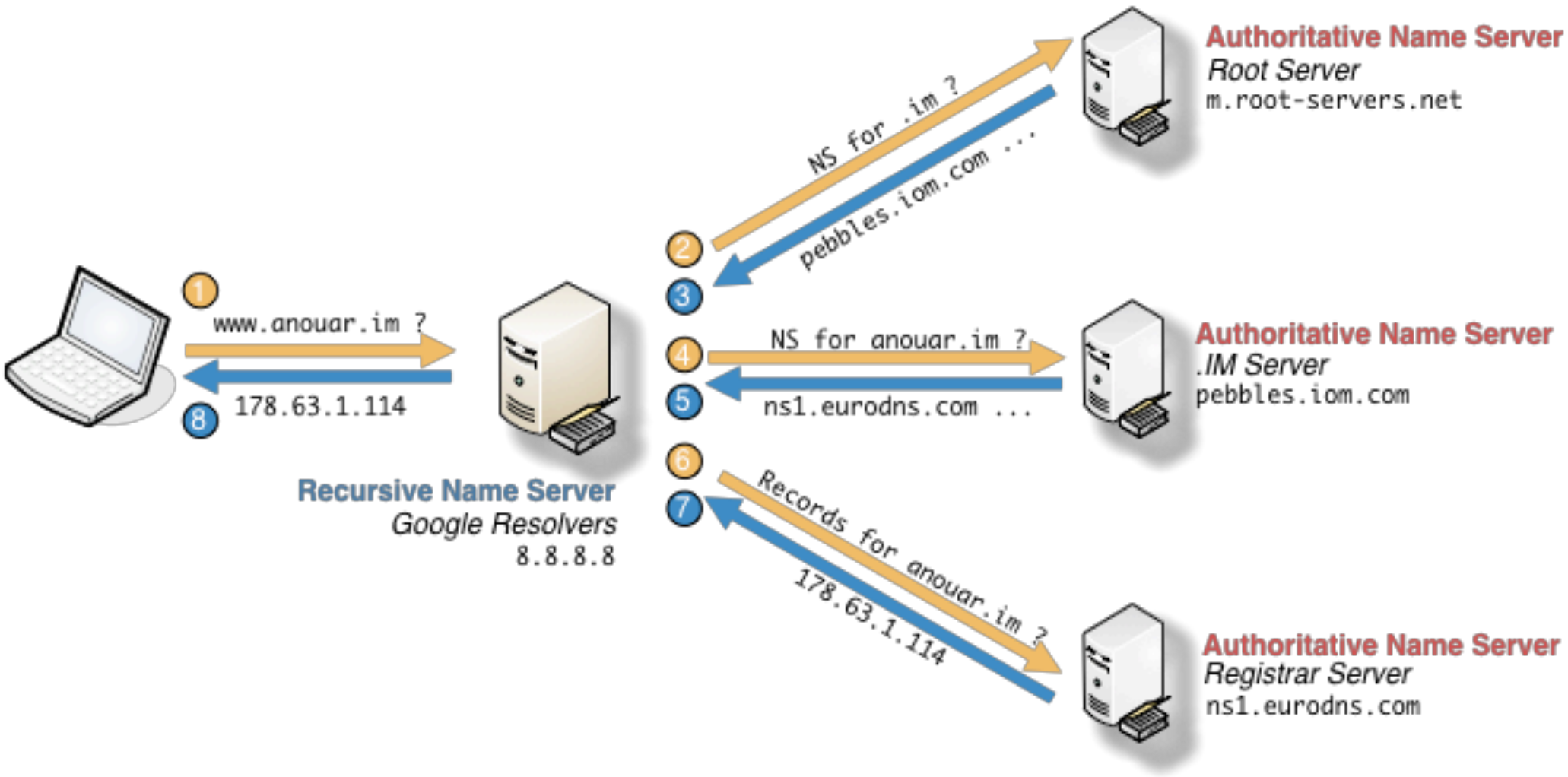
DNS

- **DNS Record:** Unit of information in DNS
  - **Type:** type of data it contains
  - **TTL:** time to live
- **A record:** IP address for a host name
- **NS record:** Name server to contact for a domain
- **MX record:** SMTP (mail) server for domain

Authorities

- A DNS server has a set of records for which it is the authoritative source

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30439
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;bob.ucsd.edu.          IN  A

;; ANSWER SECTION:
bob.ucsd.edu.       3600    IN  A   132.239.80.176

;; AUTHORITY SECTION:
ucsd.edu.       3600    IN  NS  ns0.ucsd.edu.
ucsd.edu.       3600    IN  NS  ns1.ucsd.edu.
ucsd.edu.       3600    IN  NS  ns2.ucsd.edu.
```



source: http://anouar.adlani.com/2011/12/useful-dig-command-to-troubleshot-your-domains.html

DNS Roles

- **Authoritative server:** provides authoritative information for a set of domains
  - Does not handle queries about other domains
- **Recursive resolver:** provides recursive resolution of a domain to return requested record to client
  - Handles queries about all domains
- Same protocol for both types of servers
  - Distinction is in intended purpose only

Security of DNS

- Basic DNS uses UDP without any authentication
- Man-in-the-middle attacks are possible
  - Forging response to observed query is trivial
- Off-path attacks require guessing two parameters
  - Query ID from response (16 bits)
  - Source port (approx. 15 bits)

DNSSEC

- Cryptographically sign DNS records
- Chain of trust from DNS root to subdomains, etc.
- **RRSIG:** digital signature of data
- **DNSKEY:** a public key
- **DS:** delegation record
- **NSEC:** negative response

DNSSEC Non-Properties

- Does not provide confidentiality
  - Assumes all DNS data is public
- Does not guarantee transport-layer integrity
  - Digital signatures applied to records, not packets

DNS Resource Record

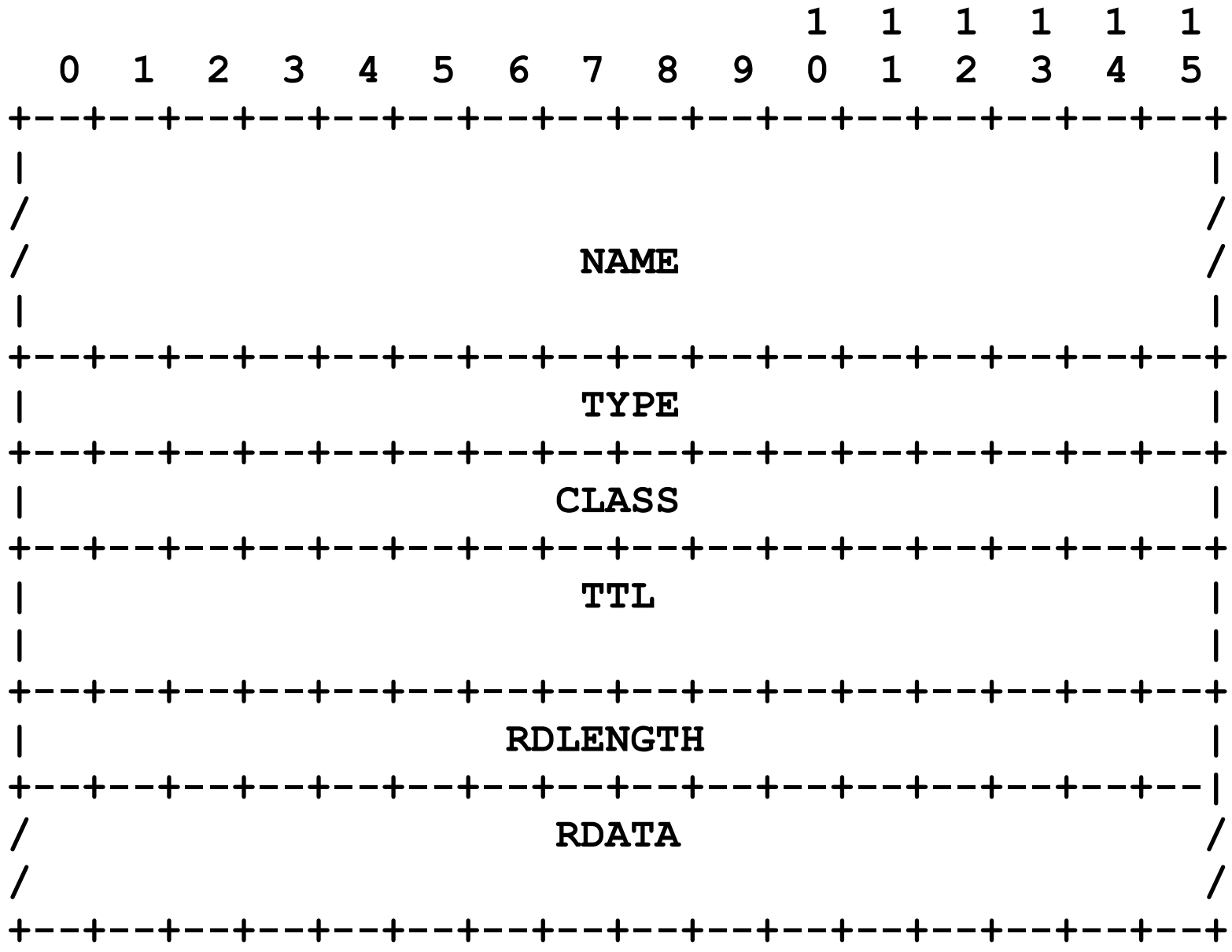
- *Typed data attached to key (name)*
- Data has a time to live (TTL)
- Basic information element in DNS

```
;; ANSWER SECTION:

www.ucsd.edu.     3600   IN A   132.239.180.101
```

name TTL type data

```
;; AUTHORITY SECTION:

  ucsd.edu.       3600   IN NS  ns-auth2.ucsd.edu.
  ucsd.edu.       3600   IN NS  ns-auth3.ucsd.edu.
```

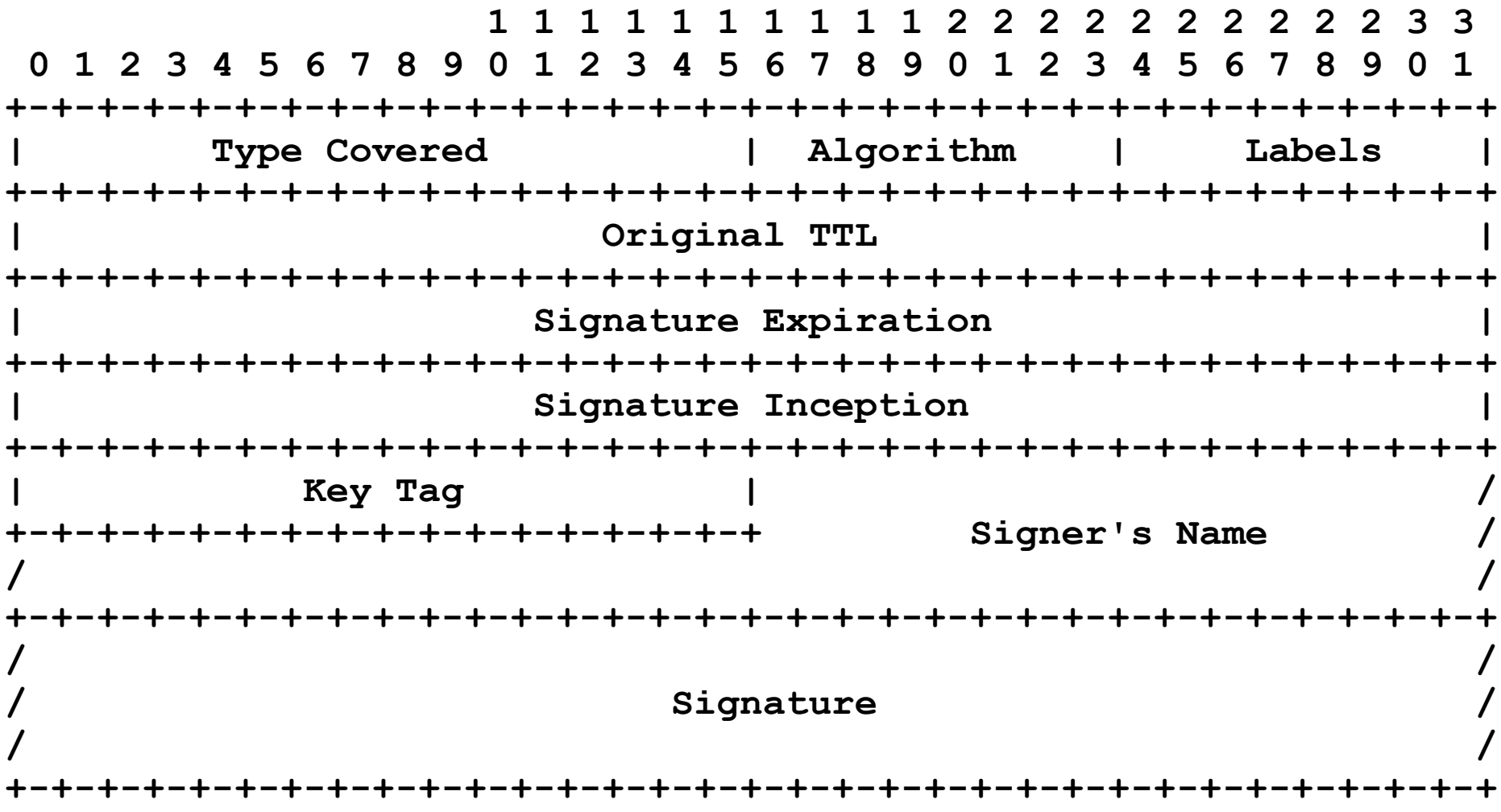
DNS Resource Record



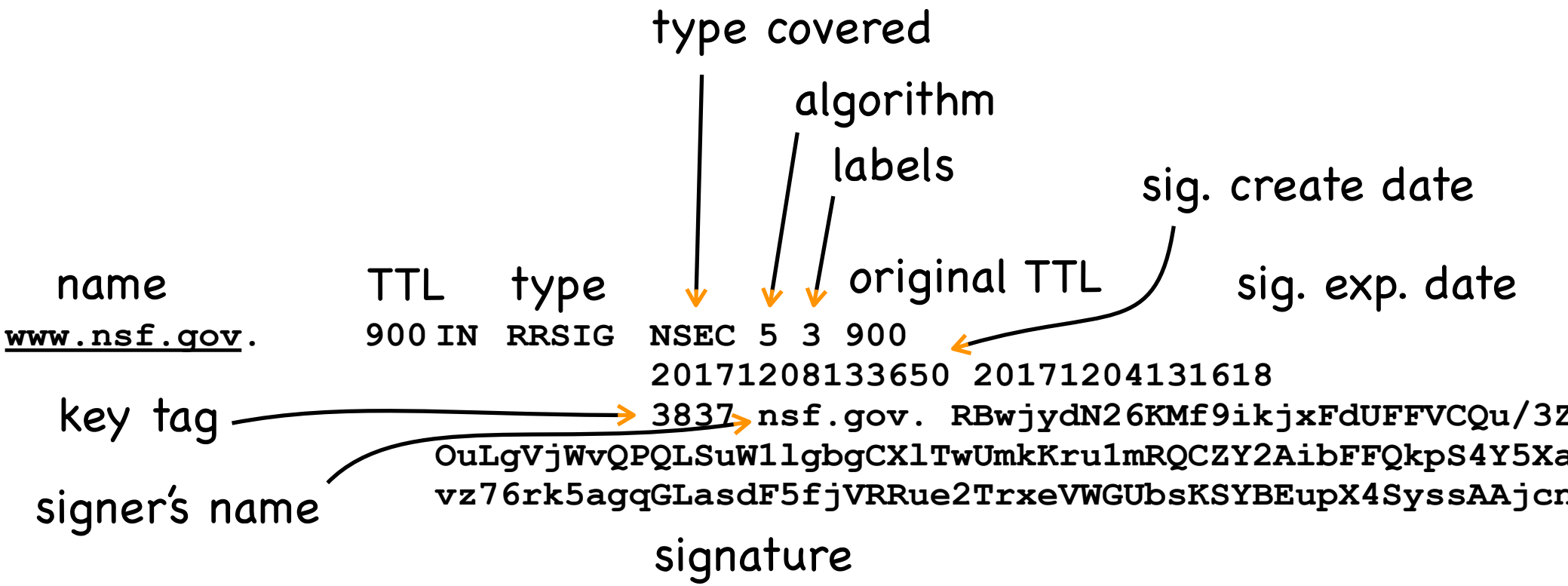
RRSIG

- *Digital signature on a resource record set*
- Signed by owner of zone (e.g. `ucsd.edu` or `edu`)
- RRSIG on a RRset protects its integrity

RRSIG RDATA


0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type Covered
Algorithm
Labels
Original TTL
Signature Expiration
Signature Inception
Key Tag
Signer's Name
Signature

RRSIG


type covered
algorithm
labels
sig. create date
name
TTL
type
original TTL
sig. exp. date
www.nsf.gov.
900 IN RRSIG NSEC 5 3 900
20171208133650 20171204131618
key tag
3837 nsf.gov. RBwjydN26KMf9ikjxFdUFFVCQu/3Z
OuLgVjWvQPQLSuW1lgbgCXlTwUmkKru1mRQCZY2AibFFQkpS4Y5Xa
signer's name
vz76rk5agqGLasdF5fjVRRue2TrxeVWGUbsKSYBEupX4SyssAAjcn
signature

Signature Algorithms

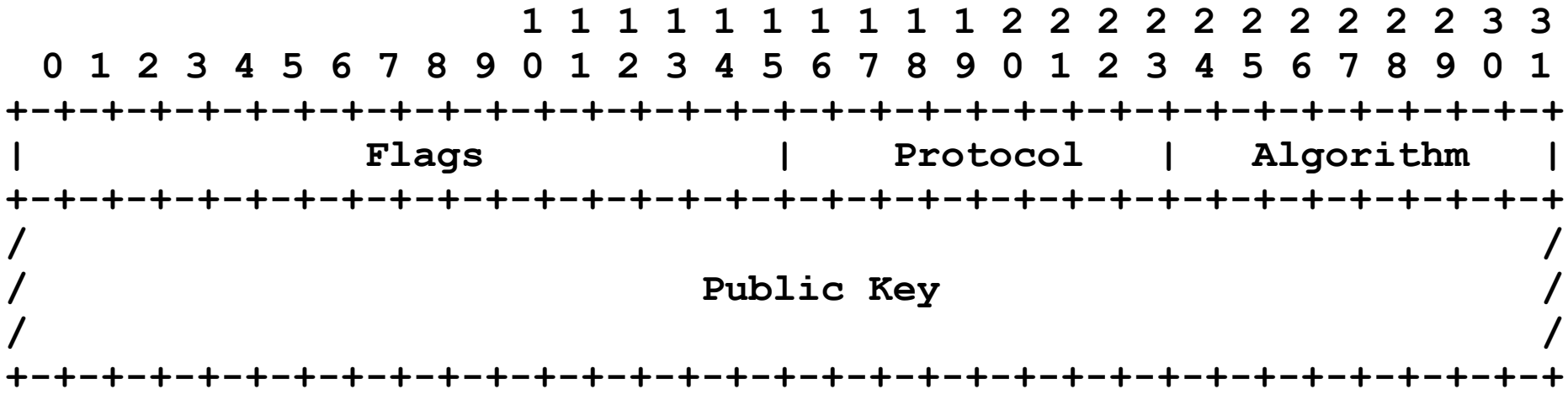
Value	Algorithm [Mnemonic]	Zone Signing	References	Status
0	reserved			
1	RSA/MD5 [RSAMD5]	n	[RFC2537]	NOT RECOMMENDED
2	Diffie-Hellman [DH]	n	[RFC2539]	-
3	DSA/SHA-1 [DSA]	y	[RFC2536]	OPTIONAL
4	Elliptic Curve [ECC]		TBA	-
5	RSA/SHA-1 [RSASHA1]	y	[RFC3110]	MANDATORY
252	Indirect [INDIRECT]	n		-
253	Private [PRIVATEDNS]	y	see below	OPTIONAL
254	Private [PRIVATEOID]	y	see below	OPTIONAL
255	reserved			

RRSIG

- *Digital signature on a resource record set*
  - All records of the same type and class for name
- Signed by owner of zone (e.g. `ucsd.edu` or `edu`)
- RRSIG on a RRset protects its integrity
- Why sign entire RRset (rather than individual RRs)?

DNSKEY

- Public signing key for zone
- Used to sign RRsets in zone
- Key tag (used in RRSIG, NSEC) calculated from key



DNSKEY

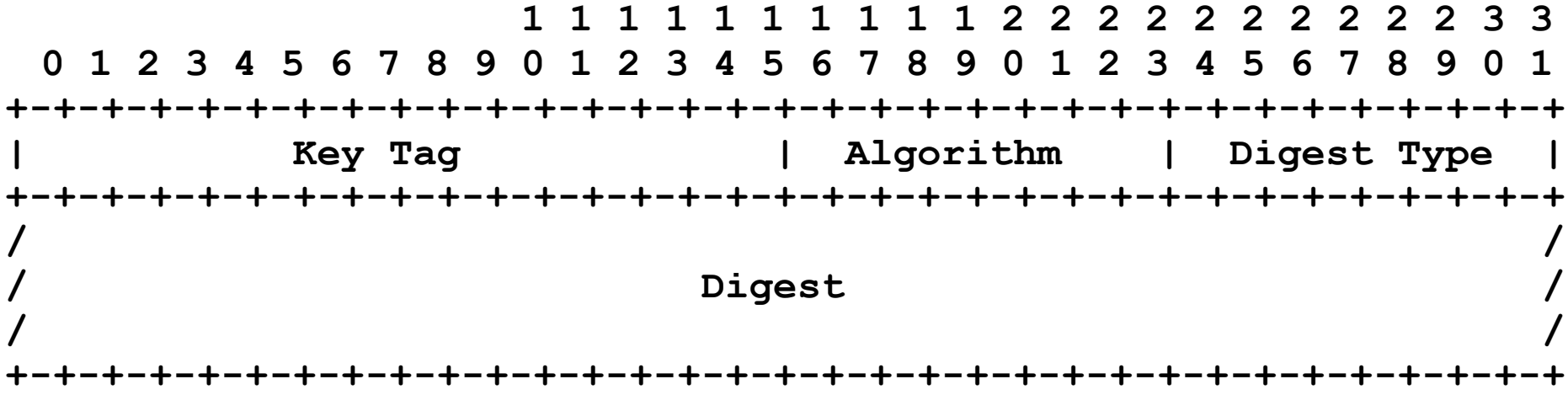
protocol (must be 3)

name	TTL	type	algorithm	key

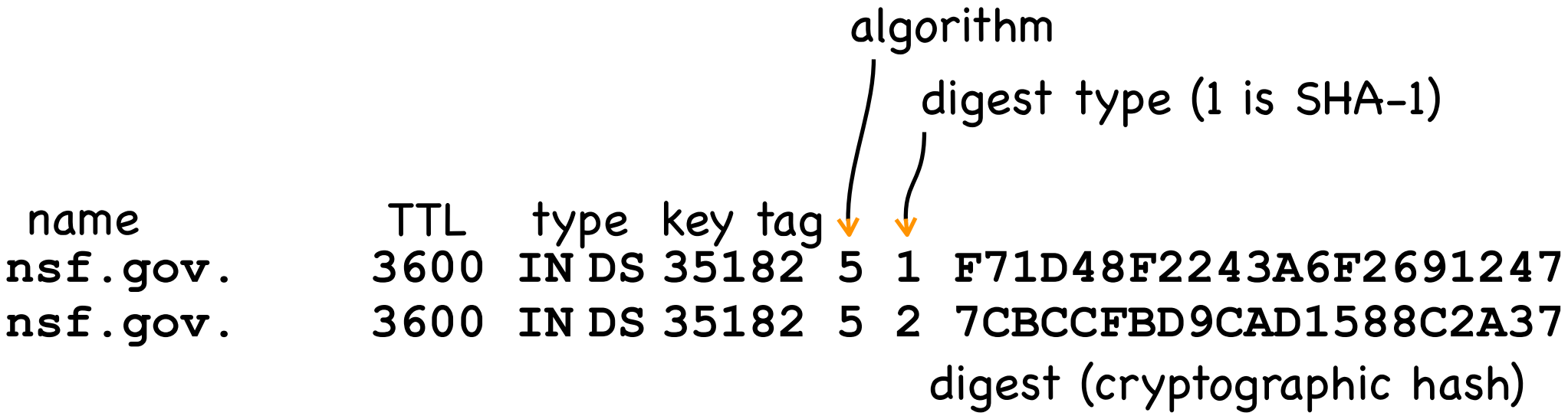
```
nsf.gov.      172800 IN  DNSKEY 257 3 5 AwEAAdEvT5jUn1aZCohFHYf4seSCVMSOtq
+fd1xN8CiLbTmHLphZpn/wA0cRUikobH5YQ8TQw FitV8fOh6deXDH6s/KReVFqMprtrtbQ4
0hj9C7UEdiPfM0QZdZjPTEXBnvTV4f20oGMgYZEQuMan 6jtwHHoq/8uuIv2A16zxeA1ynJ3
tgqIq3PMKksgIH5W05UNQoF9m9ArEIy6q70jpWr5N2ZYDNc0J 52ovSZvzrvM=
```

DS

- Delegates authority for a zone
- Specifies the key (DNSKEY) to be used to sign zone
- Accompanies NS record in zone delegation chain

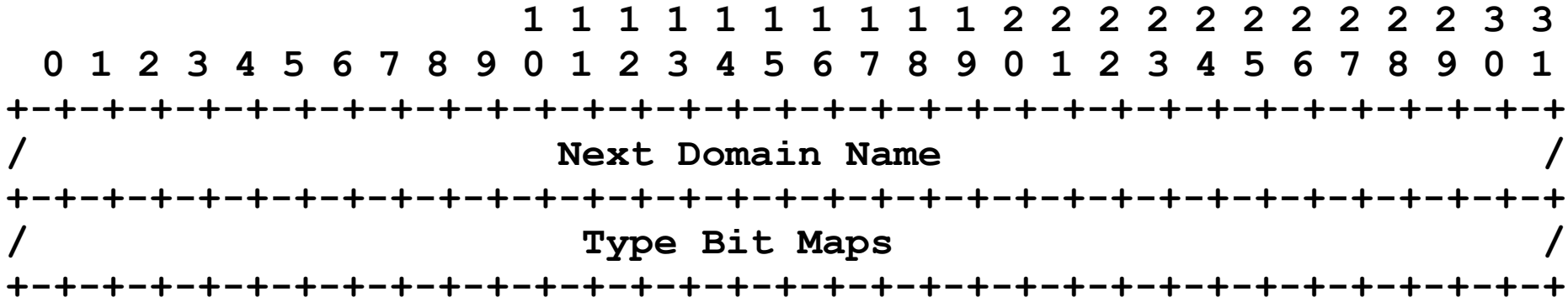


DS


algorithm
digest type (1 is SHA-1)
name TTL type key tag
nsf.gov. 3600 IN DS 35182 5 1 F71D48F2243A6F2691247
nsf.gov. 3600 IN DS 35182 5 2 7CBCCFBD9CAD1588C2A37
digest (cryptographic hash)

NSEC

- Specifies next entry in database
- Used to prove non-existence of records — *how?*



NSEC

name	TTL	type	next entry	set of types
www.nsf.gov.	**900**	**IN NSEC**	**xmpp.nsf.gov.**	**A AAAA RRSIG NSEC**

NSEC3

- NSEC allows anyone to enumerate zone (find all records)
  - Why is this a problem?
- NSEC3 uses hash of next record