isec
INFORMATION SECURITY
lectures by Ferucio Laurentiu Tiplea

Security Extensions for DNS

DNSsec

Prof.dr. Ferucio Laurențiu Țiplea

Fall 2023

Department of Computer Science
"Alexandru Ioan Cuza" University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Short introduction to DNS

Domain Name System

1. Internet domain
   - Is a collection of data+ describing a self-contained administrative and technical unit on the Internet;
   - Can comprise computer addresses, services (such as e-mail or FTP), resource (such as hypertext documents), and more;
2. Domain name = identification string for an Internet domain;
3. Domain Name System (DNS) = hierarchical and decentralized naming system for Internet domains.

DNS is the "phone-book" of the Internet!

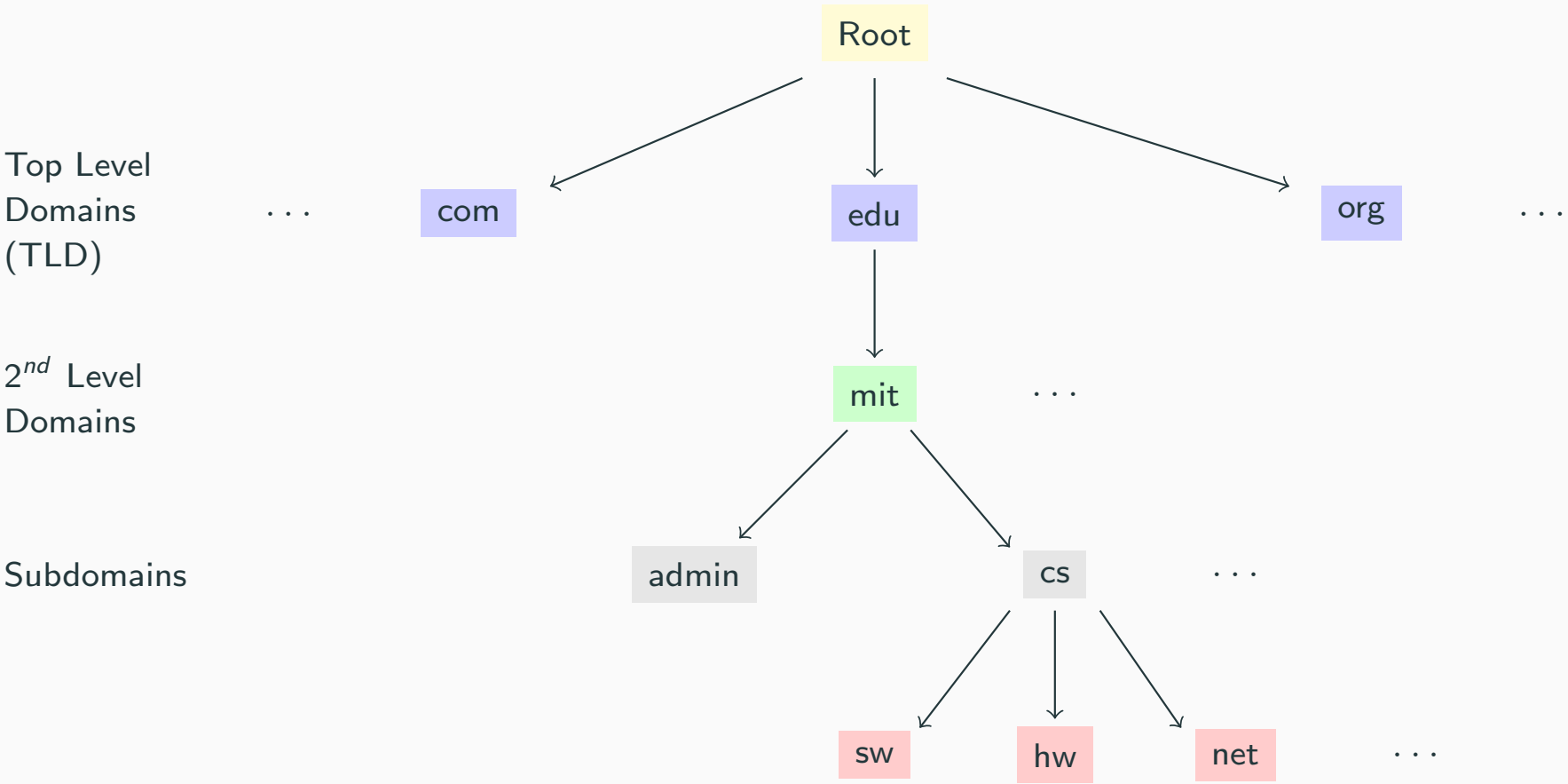
Domain Name System

1. DNS was proposed in the early 1980s by Paul V. Mockapetris;
2. DNS original specifications were published in 1983 in RFC 882 and RFC 883;
3. DNS became an Internet Standard in 1986 (RFC 1034 and RFC 1035).

The DNS has three major components:

1. The domain name space and resource records = set of information tree-like structured;
2. Name servers = server programs which hold information about the domain tree's structure and set information;
3. Resolvers = programs that extract information from name servers.

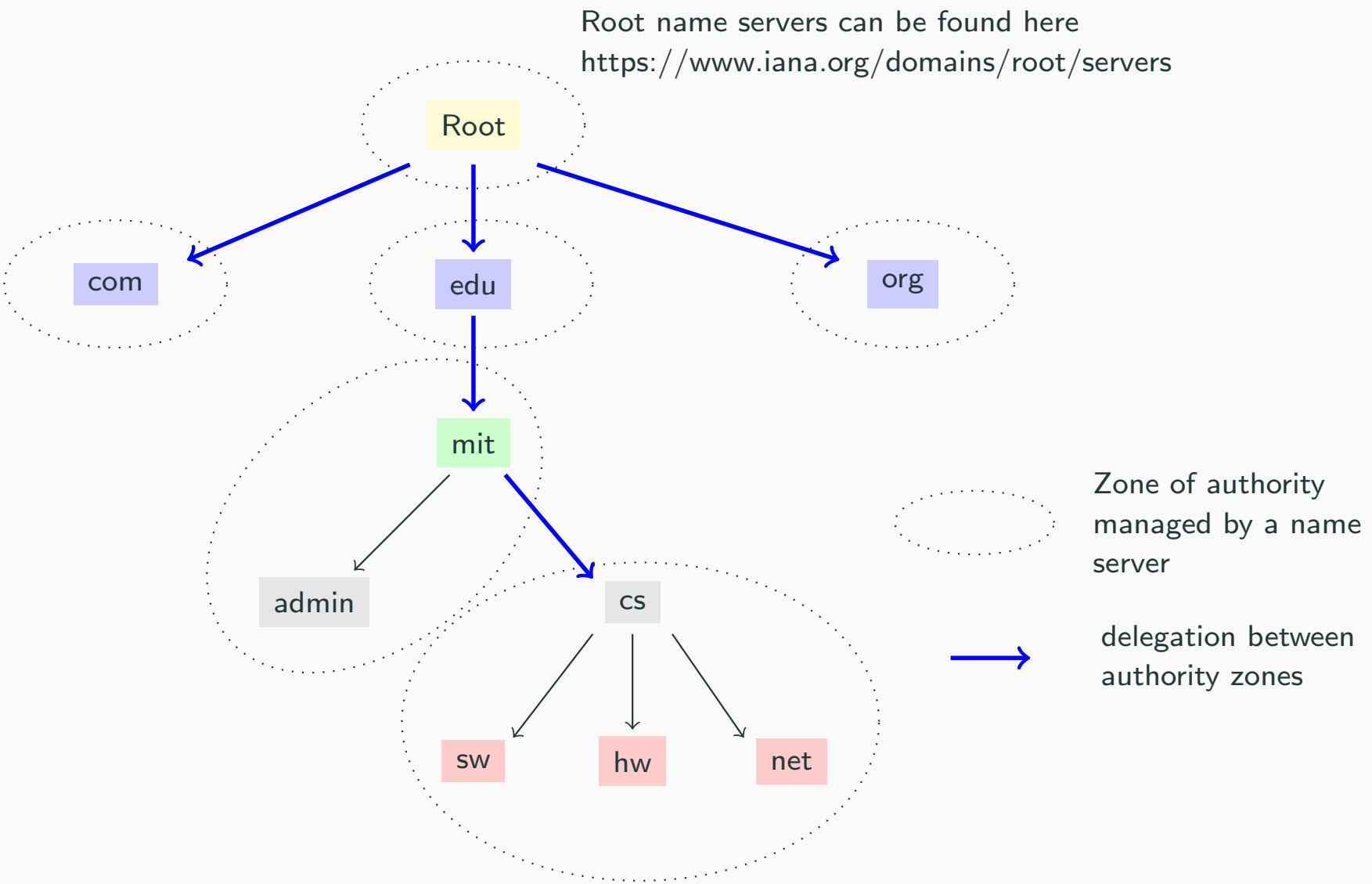
DNS domain name space



Zones of authority and name servers

1. The DNS name space is comprised logically of domain names but physically of zones;
2. Zones are obtained by making cuts between adjacent nodes of the DNS name tree to create groups of contiguous nodes in the tree;
3. Each group is called a zone of authority;
4. Each zone is usually identified by the domain name of the highest level node in the zone;
5. The zones are non-overlapping;
6. Every zone is managed by one or more pairs (primary/master, secondary/slave) of authoritative name servers;
7. A name server may be authoritative for more than one zone.

Zones of authority and name servers



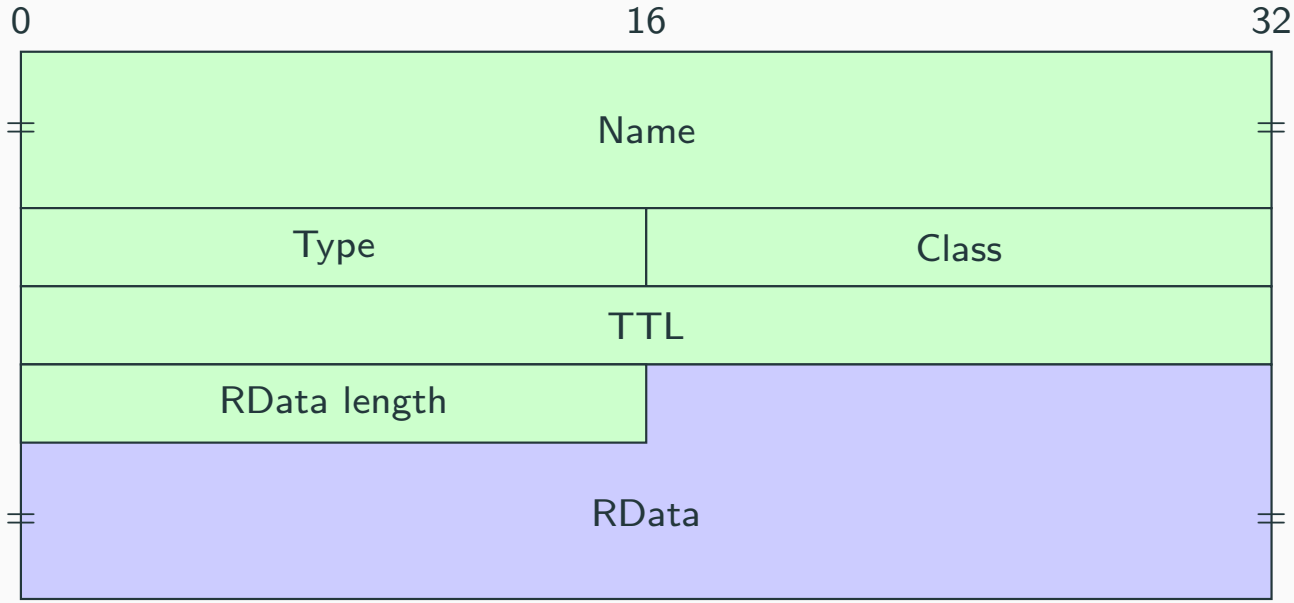
Resource Records (RR)

1. Each node in the DNS name tree has associated a number of records, usually called resource records (RR), depending on the node type;

2. The RRs are added, changed, or deleted when DNS information changes (this is done by administrators);

3. The set of all RRs gives rise to a distributed database that is structured in a hierarchy comparable to the hierarchy of authorities.

RR format



- Name = domain name where the RR is found (RR's owner)
- Type = type of RR
- Class = identifies a protocol family or instance of a protocol (mostly, IN for Internet)
- TTL = time to live (time to cache an RR) in seconds (primarily used by resolvers)
- RData length = length of RData field
- RData = resource data

Some DNS RR types

SOA = Start Of Authority

- Every zone has exactly one SOA RR, at the beginning of the zone;
- It holds information about the zone, such as:
  - Default TTL for everything in the zone;
  - Primary name server;
  - The e-mail address of the person responsible for administering the domain's zone file.

Example 1

```
google.com.        900    IN    SOA    ns1.google.com
                                       dns-admin.google.com
                                       494510988  900  900  1800  60
```

TTL = 900
NS = ns1.google.com
e-mail = dns-admin@google.com

Some DNS RR types

NS = Name Server

- Specifies the name of the authoritative DNS name server for the zone;
- Each zone must have at least one NS RR that points to its primary name server, and that name must also have a valid A RR.

A = Address

- Contains a 32-bit IP address (it is the IP address of the node, stored for the resolution process).

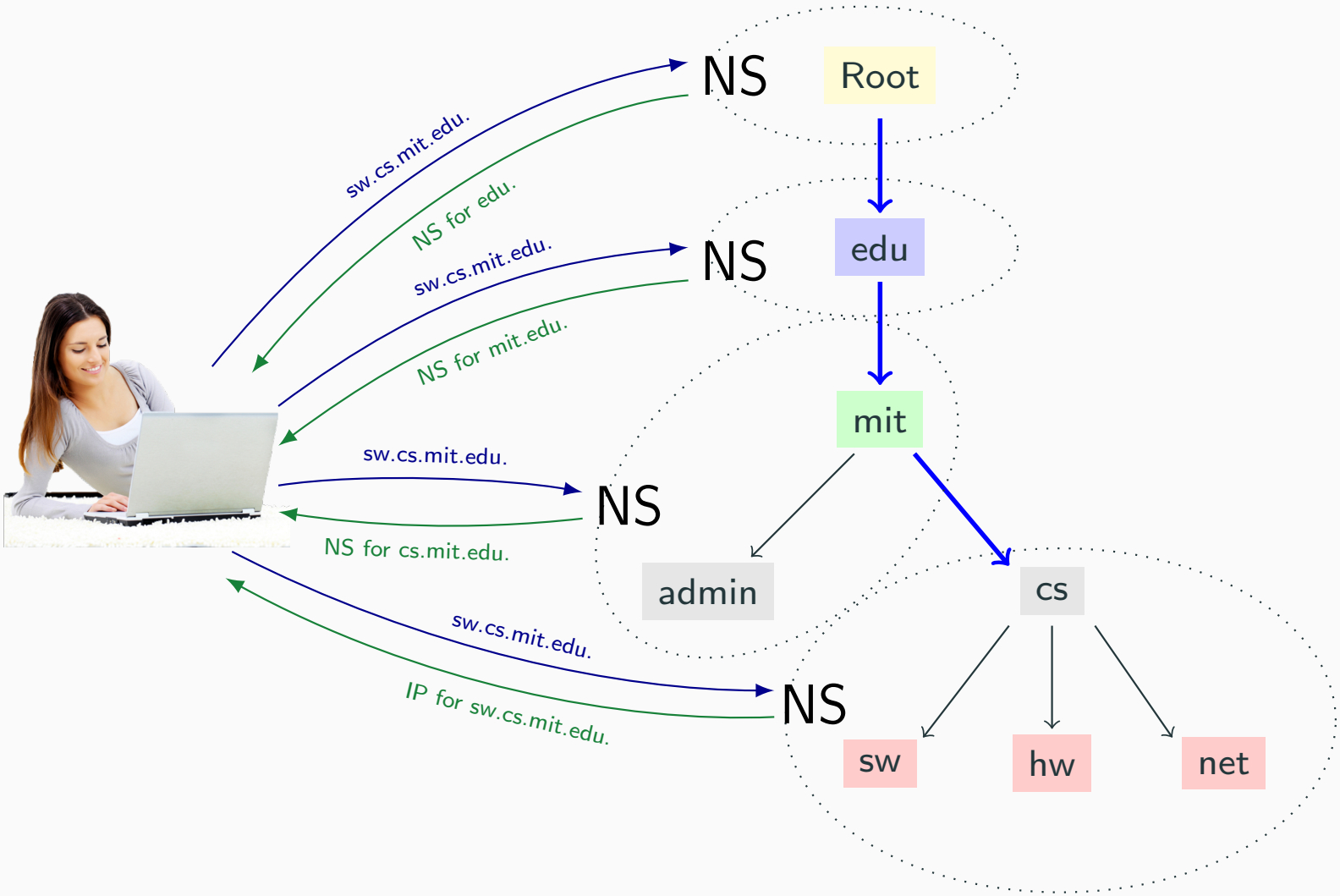
MX = Mail eXchanger

- Specifies the location (device name) that is responsible for handling e-mail sent to the domain, and that location must have a valid A RR.

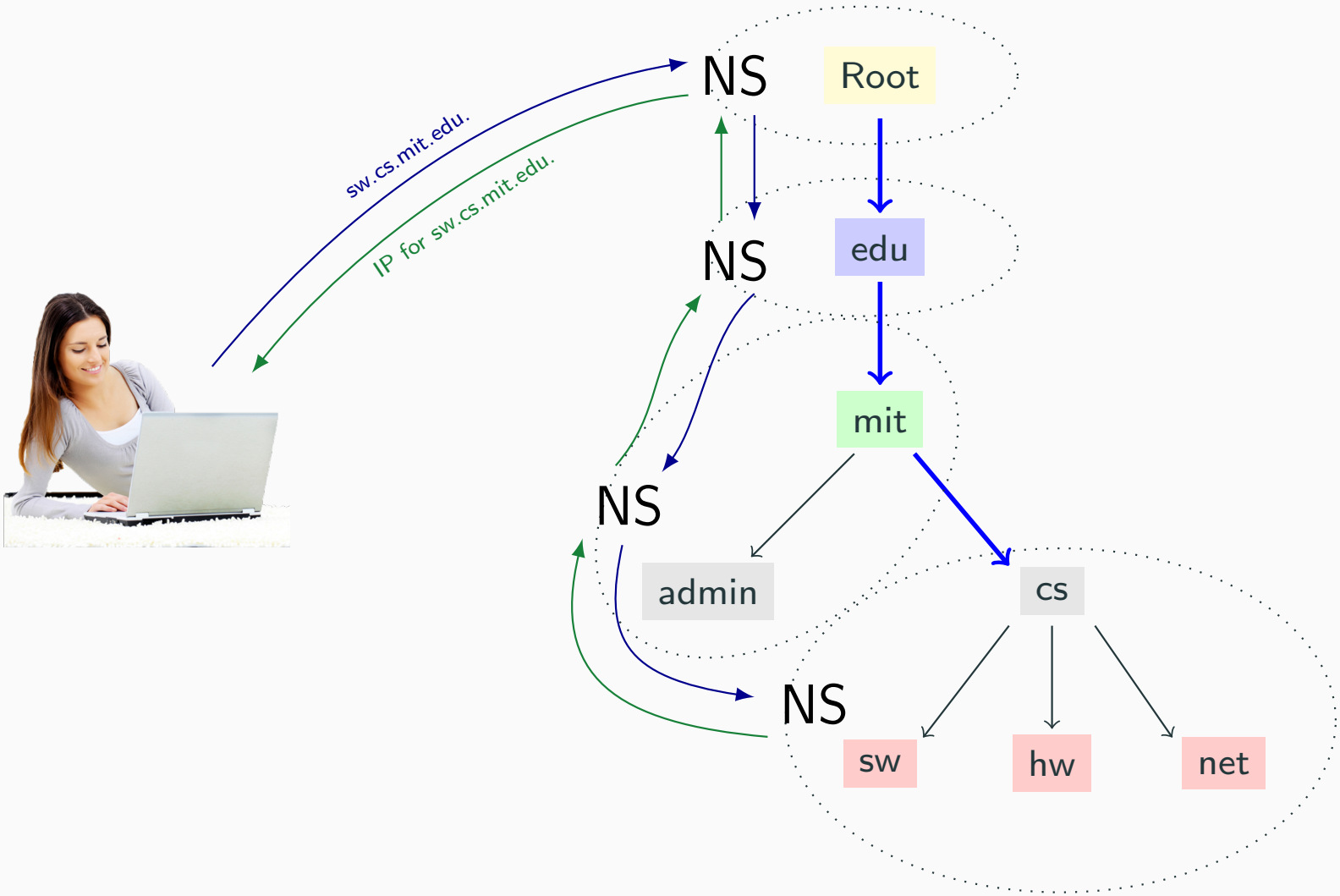
DNS resolution

1. Most typical types of resolution:
   - 1.1 (Standard) name resolution = determine the IP address of a domain name;
   - 1.2 Reverse name resolution = determine the domain name associated with an IP address;
   - 1.3 e-mail resolution = determine where to send the e-mail messages based on the e-mail address used in a message;
2. DNS name resolution techniques:
   - 2.1 Iterative resolution;
   - 2.2 Recursive resolution (not all name servers support recursion, especially servers near the top of the hierarchy).

Iterative resolution



Recursive resolution



Resolvers and DNS transport

Types of resolvers:

1. Full resolver;
2. Stub resolver.

DNS transport:

1. By UDP for conventional queries;
2. By TCP for zone transfer.

What is DNSsec?

DNS vulnerabilities

S. Bellovin: *Using the Domain Name System for System Break-ins*, Proceedings of the Fifth USENIX UNIX Security Symposium Salt Lake City, Utah, June 1995

Author's note: "... this paper has been withheld by the author for over four years ... because it described a serious vulnerability for which there was no feasible fix. The only choice would have been to give up entirely on name based authentication, a choice the industry was not able to make in 1990."

- DNS snooping
- DNS ID hacking
- DNS cache poisoning

What is DNSsec?

1. After Bellovin's paper, securing DNS became a fundamental issue;
2. Proposed DNSsec standards: RFC 4033, 4034, 4035 (in 2005).

DNSsec is an extension of DNS that adds:

- Data origin authentication – allows a resolver to cryptographically verify that the data it has received actually came from the zone where it believes the data originated;
- Data integrity protection – allows the resolver to know that the data has not been modified in transit since it was originally signed by the zone owner with the zone's private key.

DNSsec specific elements

New RR types

DNSsec uses four new types of RRs:

- RRSIG (RR SIGnature) – stores a digital signature over an RRset;
- DNSKEY (DNS public KEY) – stores a public key for digital signature verification;
- NSEC/NSEC3 (Next SECure) – used to prove that something really does not exist;
- DS (Delegation Signer)– stores a hash value of a verification public key.

DNSsec signature algorithms (RFC 8624)

Number	Mnemonics	Signing	Verification
1	RSAMD5	must not	must not
3	DSA	must not	must not
5	RSASHA1	not recommended	must
6	DSA-NSEC3-SHA1	must not	must not
7	RSASHA1-NSEC3-SHA1	not recommended	must
8	RSASHA256	must	must
10	RSASHA512	not recommended	must
12	ECC-GOST	must not	may
13	ECDSAP256SHA256	must	must
14	ECDSAP384SHA384	may	recommended
15	ED25519	recommended	recommended
16	ED448	may	recommended

A combination like "not recommended – must" means that validators must implement it in order to validate/invalidate existing RRSIGs, but it is not recommended to use it to sign new RRsets.

DNSsec digest algorithms (RFC 8624)

Number	Mnemonics	Signing	Verification
1	SHA-1	must not	must
2	SHA-256	must	must
3	GOST R 34.11-94	must not	may
4	SHA-384	may	recommended

Remarks:

1. SHA-256 is widely used and considered strong;
2. GOST R 34.11-94 has been superseded by GOST R 34.11-2012 in RFC 6986. GOST R 34.11-2012 has not been standardized for use in DNSsec.

Canonical ordering of DNS names (RFC 4034)

For the purposes of DNSsec:

1. Owner names are ordered by treating individual labels as unsigned left-justified octet strings;
2. The absence of a octet sorts before a zero value octet;
3. Uppercase US-ASCII letters are treated as lowercase;
4. Start by sorting the names according to their rightmost labels;
5. For names in which the most significant label is identical, continue sorting according to their next most significant label, and so forth.

---

example
a.example
yljkjljk.a.example
Z.a.example
zABC.a.EXAMPLE

z.example
\001.z.example
*.z.example
\200.z.example

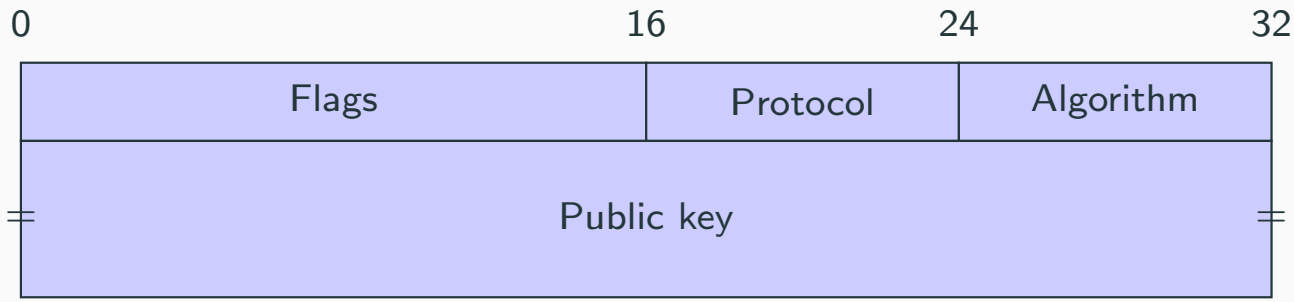
Canonical RR ordering in an RRset (RFC 4034)

For the purposes of DNSsec:

1. RRs with the same owner name, class, and type are sorted by treating the RDATA portion of the canonical form of each RR as a left-justified unsigned octet sequence in which the absence of an octet sorts before a zero octet;

2. If a DNSsec implementation detects duplicate RRs when putting the RRset in canonical form, it must treat this as a protocol error or remove all but one of the duplicate RR(s) for the purposes of calculating the canonical form of the RRset.

RData for DNSKEY



- Flags = used to differentiate between classes of pairs of keys (see next slide)
- Protocol = must have value 3; otherwise, is treated as invalid
- Algorithm = identifies the public key's cryptographic algorithm (e.g., 5 stands for RSA/SHA-1)
- Public key = holds the public key material

ZSK vs. KSK

Public keys in DNSsec have two fundamental uses: to sign a zone, called in this case zone signing keys (ZSK), and to validate a ZSK, called in this case key signing keys (KSK).

The "flags" field differentiates between the two classes of keys:

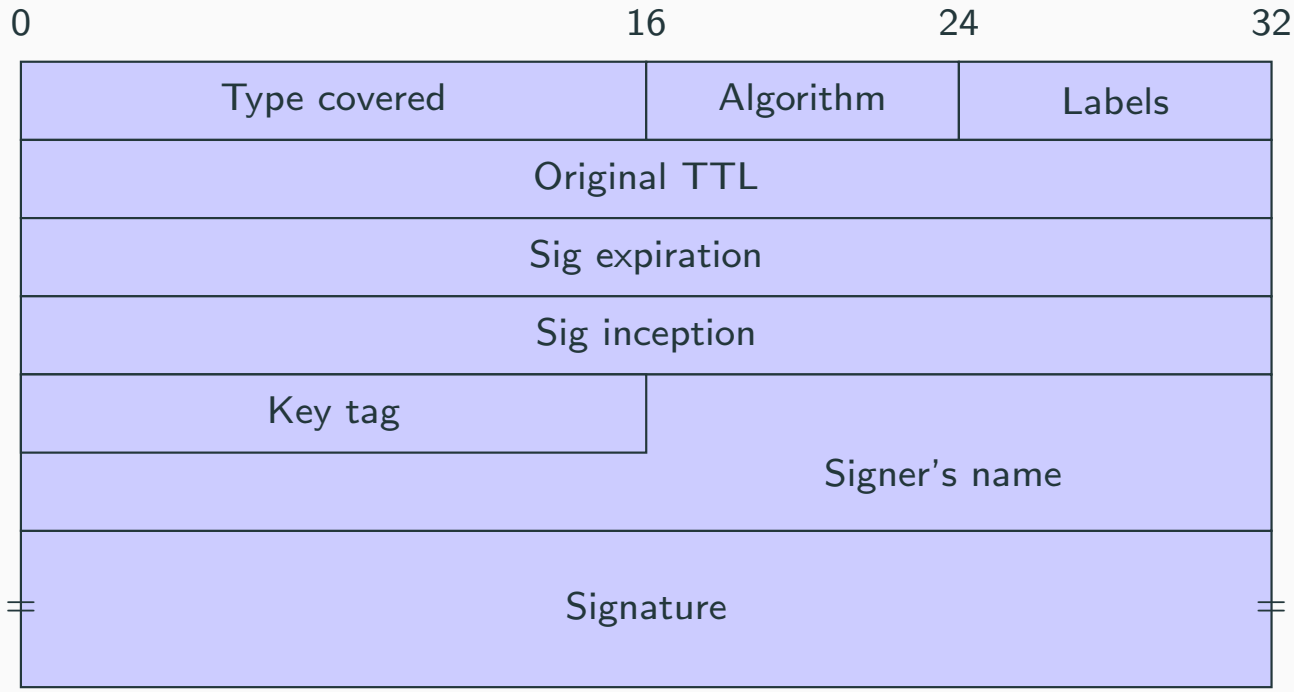
1. If flag 7 is 1, the key is used for signing the zone;
2. If flag 15 is 1, the key is used to validate a ZSK.

Example 2

When the flags field value is 256 (meaning that only flag 7 is 1), the key is for zone signing, and when it is 257 (both flags 7 and 15 are 1), the key is both for zone and key signing.

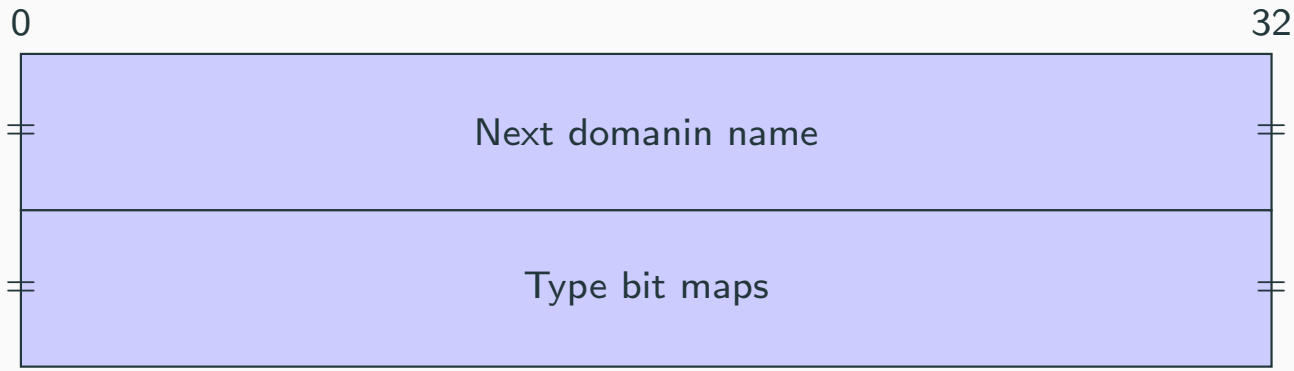
KSKs are used to validate ZSKs and create a chain of trust starting from the root to the desired node.

RData for RRSIG



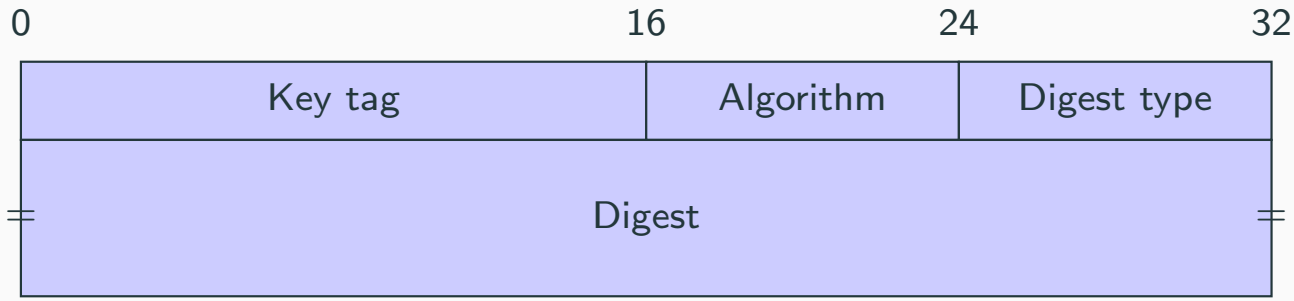
- Original TTL = the TTL of the covered RRset
- Signer's name = must contain the name of the zone of the covered RRset
- Key tag = the key tag value of the DNSKEY RR that validates this signature (see RFC 4034 for calculation of Key Tag values)

RData for NSEC



- Next domain name = the next owner name (in the canonical ordering of the zone) that has authoritative data or contains a delegation point NS RRset
- Type bit maps = identifies the RRset types that exist at the NSEC RR's owner name

RData for DS



- Key tag = the key tag of some DNSKEY RR (corresponding to some KSK)
- Algorithm = the algorithm number of some DNSKEY RR
- Digest type = identifies the algorithm used to construct the digest
- Digest = includes a digest of that DNSKEY RR

Zone signing

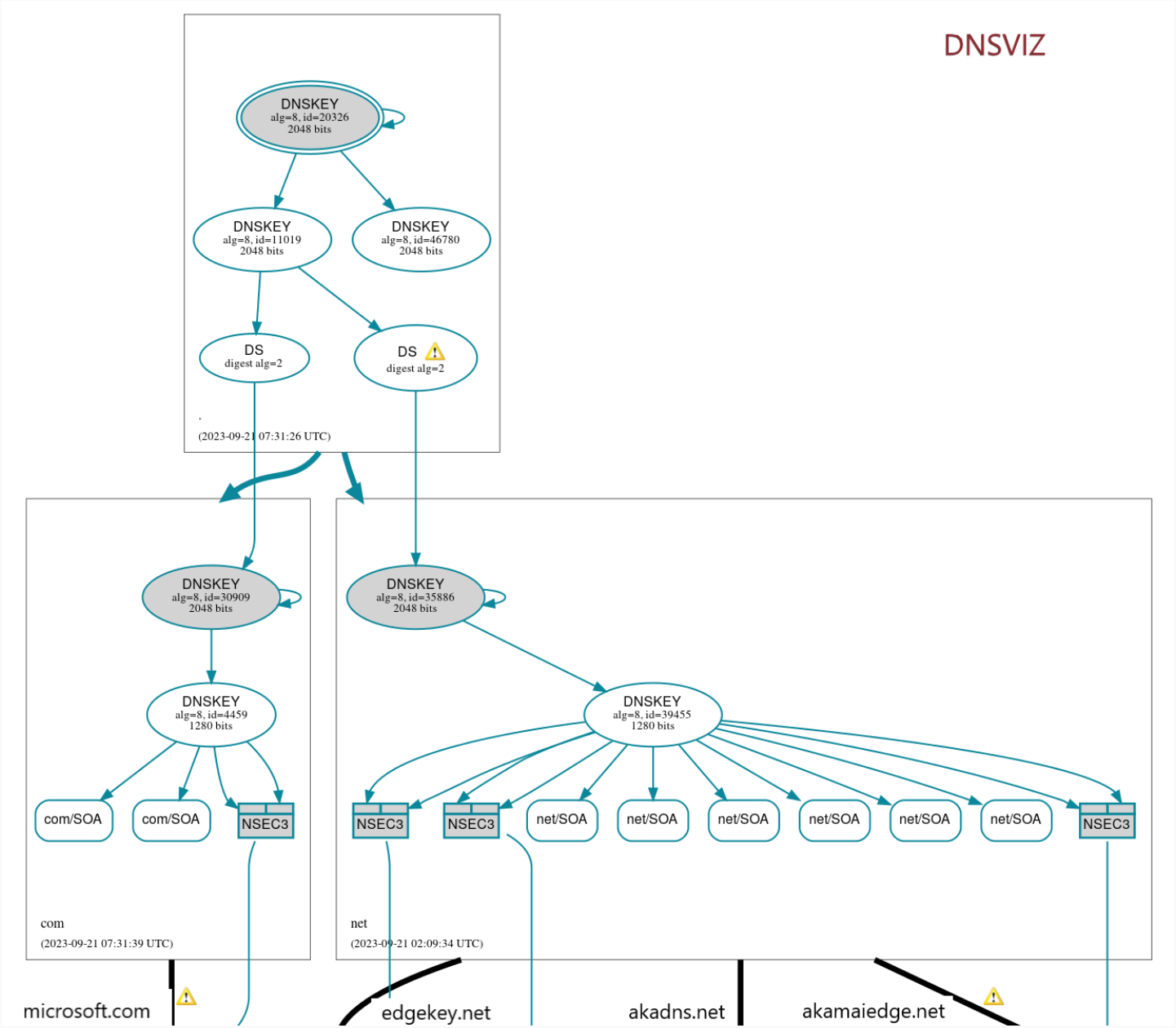
Zone signing

To sign a zone means to include DNSKEY RRs, RRSIG RRs, NSEC RRs, and optionally DS RRs in that zone, according to the following rules:

- To sign a zone, zone's admin generates one or more (public,private) keys and uses the private keys to sign authoritative RRsets. For each private key used to create RRSIG RRs, a corresponding DNSKEY RR should be included in the zone;
- Suppose the signed zone must be linked to the parent zone. In that case, the zone validation keys (DNSKEY RRs) must be signed by a KSK, its verification key (of DNSKEY RRs) must be present in the zone, and a DS RR of it must be in the parent zone at the delegation point (separation entry point);
- Each owner name in the zone that has authoritative data or a delegation point NS RRset, must have an NSEC resource record.

More on zone signing can be found in RFC 4035.

Zone signing



Resolving and authenticated DNS response

Resolving and authenticated DNS response

In class by means of examples:

- DNSsec_Example1.pdf – for zone signing
- DNSsec_Example2.pdf – for resolving and responses

Zone enumeration

Zone enumeration

The NSEC RR introduces a side-effect in that the contents of a zone can be enumerated:

- An NSEC record lists two names that are ordered canonically, in order to show that nothing exists between the two names;
- The complete set of NSEC records lists all the names in a zone;
- To enumerate the content of a zone, query for names that do not exist!

The enumeration of a zone can be used:

- As a source of probable e-mail addresses for spam, or
- As a key for multiple WHOIS queries to reveal registrant data that many registries may have legal obligations to protect.

Delegation to unsigned zones

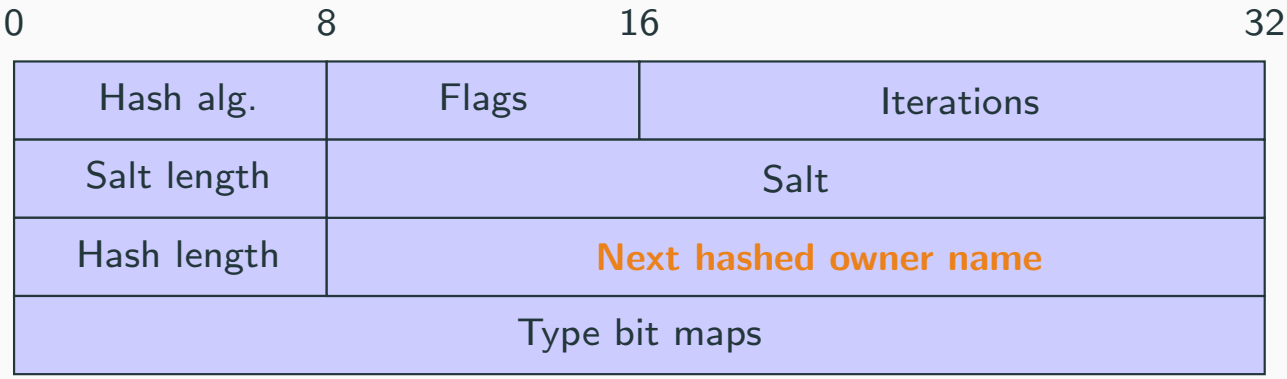
The cost of a secure delegation (with DS) to unsigned areas can be high in some instances, such as:

- Large delegation-centric zones;
- Zones where insecure delegations are updated rapidly.

In cases cases, the costs of maintaining an NSEC RR chain may be extremely high.

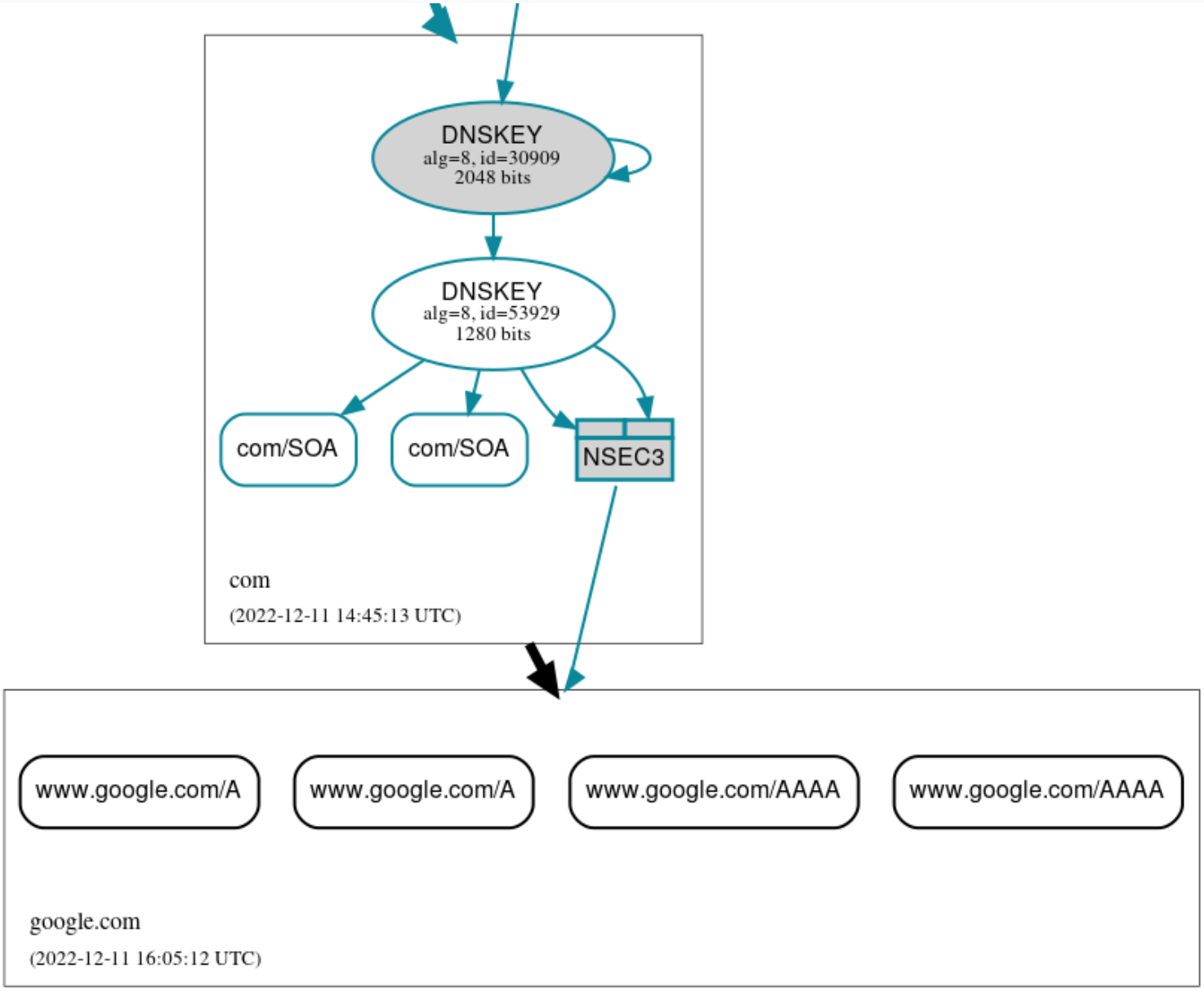
RData for NSEC3

NSEC3 was introduced in RFC 5155 to address the two previously mentioned problems (zone enumeration and the cost of delegation to unsigned zones).



The last bit of the Flags field is called the Opt-Out flag. It tells whether the NSEC3 RR is for all delegations or only for secure delegations (see RFC 5155 for details).

NSEC3 delegation



Concluding remarks

Concluding remarks

- DNSsec is a critical service on the Internet;
- ICANN has been supporting DNSsec deployment for many years through various initiatives and capacity-building programs;
- According to APNIC, only 30% of the world has achieved DNSsec validation;
- Countries with exceptionally high validation rates: Saudi Arabia (98%), Finland (94%), Iceland (88%), Norway (86%), and Sweden (86%);
- Despite the slow adoption, DNSSEC remains the only real option for preventing cache poisoning attacks.

The slow deployment of DNSsec is due to the lack of knowledge about the security problems generated by DNS and the lack of requirements for implementing this technology.