Security Extensions for DNS

DNSsec

Prof.dr. Ferucio Laurențiu Țiplea

Fall 2021

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

e-mail: ferucio.tiplea@uaic.ro

Outline

Short introduction to DNS

What is DNSsec?

DNSsec specific elements

Zone signing

Resolving and authenticated DNS response

Short introduction to DNS

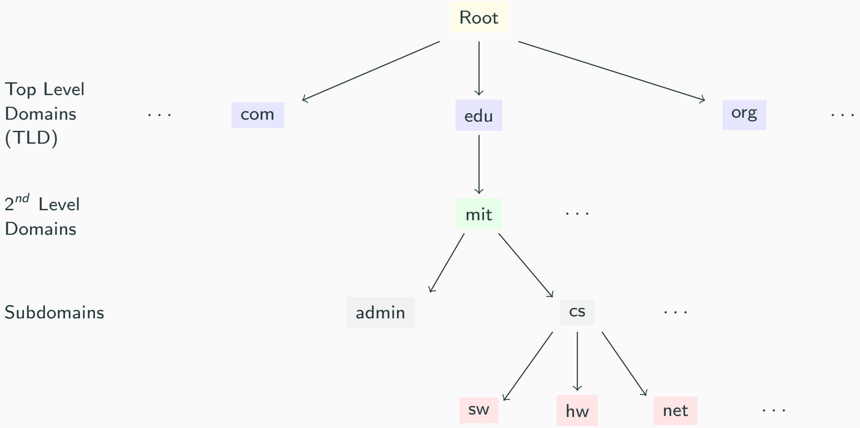
Domain Name System

1. Internet domain = collection of data describing a self-contained administrative and technical unit on the Internet
2. An internet domain can comprise computer addresses, services (such as e-mail or FTP), resource (such as hypertext documents), and more
3. Domain name = identification string for a domain
4. Domain Name System (DNS) = hierarchical and decentralized naming system for Internet domains
5. 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)

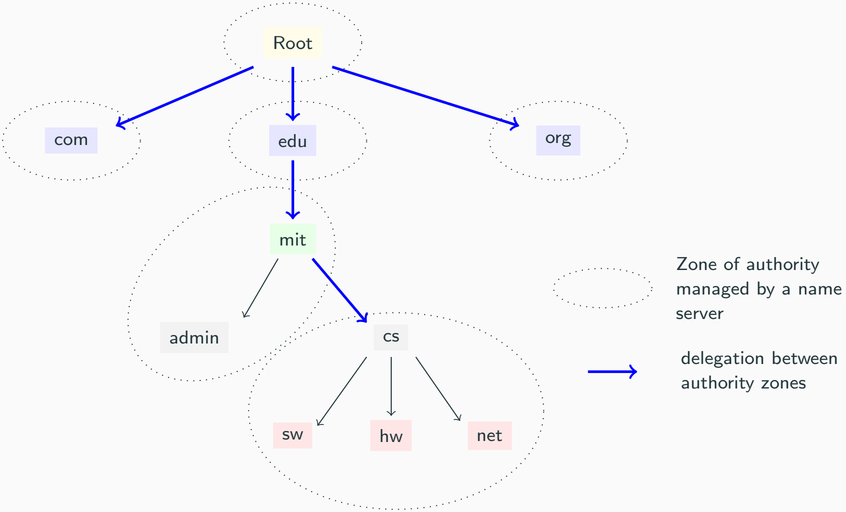
DNS domain name space



Zones of authority

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


Root
com
edu
org
mit
admin
cs
sw
hw
net
Zone of authority managed by a name server
delegation between authority zones

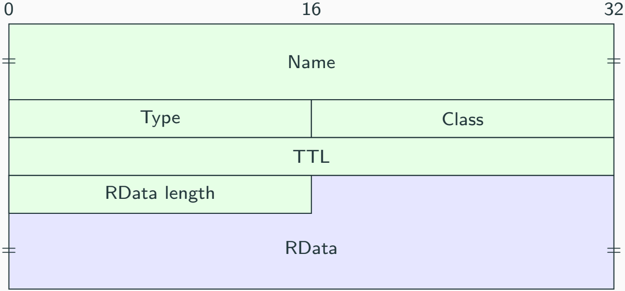
Resource Records (RR)

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



0 16 32

Name

Type | Class

TTL

RData length

RData

- Name = object, domain or zone name (limited to 63 chars)
- Type = type of resource record (SOA, NS, A, MX ...)
- Class = class of resource record (mostly, IN for Internet)
- TTL = time to live (in seconds) = time to cache a record
- RData length = length of RData field
- RData = resource data

Some DNS RRs

1. A = Address
   1.1 Contains a 32-bit IP address (it is the IP address of the node, stored for the resolution process)
2. SOA = Start Of Authority
   2.1 Every zone has exactly one SOA RR, present at the beginning of the zone
   2.2 It holds information about the zone itself and about other records
3. NS = Name Server
   3.1 Specifies the name of a DNS name server that is authoritative for the zone
   3.2 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
4. MX = Mail eXchanger
   4.1 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
    1.2 Reverse name resolution
    1.3 E-mail resolution
2. DNS name resolution techniques
    2.1 Iterative resolution
    2.2 Recursive resolution

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 – stores a digital signature over an RRset
- DNSKEY – stores a public key for digital signature verification
- NSEC (NSEC3) – used to prove that something really does not exist
- DS – 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

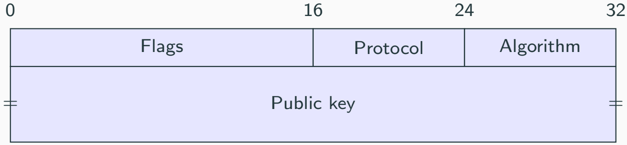
Canonical RR ordering in an RRset (RFC 4034)

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

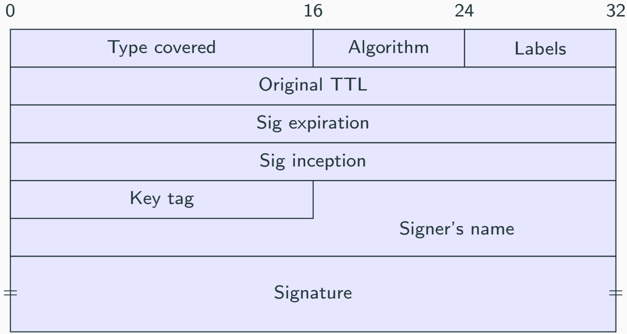
2. If a DNSsec implementation detects duplicate RRs when putting the RRset in canonical form, it must treat this as a protocol error or remove all but one of the duplicate RR(s) for the purposes of calculating the canonical form of the RRset

RData for DNSKEY



- Flags = If bit 7 has value 1, then the DNSKEY record holds a DNS zone key; otherwise, the DNSKEY record holds some other type of DNS public key
- 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

RData for RRSIG



0 16 24 32

Type covered | Algorithm | Labels

Original TTL

Sig expiration

Sig inception

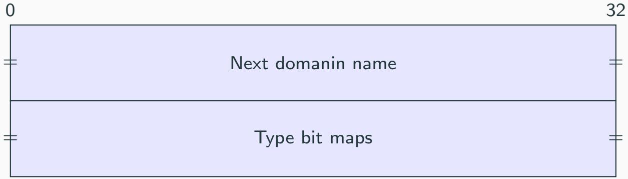
Key tag

Signer's name

Signature

- Original TTL = the TTL of the covered RRset
- Sig expiration/inception = validity period for the signature
- Key tag = the key tag value of the DNSKEY RR that validates this signature (see RFC 4034)
- Signer's name = must contain the name of the zone of the covered RRset

RData for NSEC



0

32

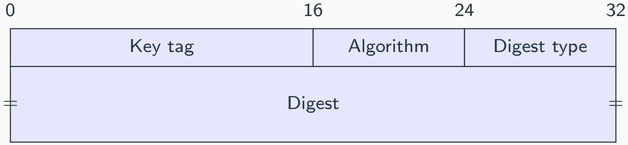
Next domanin name

Type bit maps

- 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



0 16 24 32

Key tag | Algorithm | Digest type

Digest

- Key tag = the key tag of some DNSKEY RR. It is identical to the key tag used by all RRSIG RRs that sign by the same key
- Algorithm = the algorithm number of some DNSKEY RR. It is identical to the algorithm number used by all RRSIG RRs that sign by the same key
- Digest type = identifies the algorithm used to construct the digest
- Digest = includes a digest of that DNSKEY RR.

Zone signing

Signed zone

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:

- A signed zone includes DNSKEY RRs, RRSIG RRs, NSEC RRs, and optionally DS RRs
- 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 should be included in the zone
- Each owner name in the zone that has authoritative data or a delegation point ND RRset, must have an NSEC RR
- A DS RRset should be included at a delegation point when a child zone is signed. DS RRs establish authentication chains between zones

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