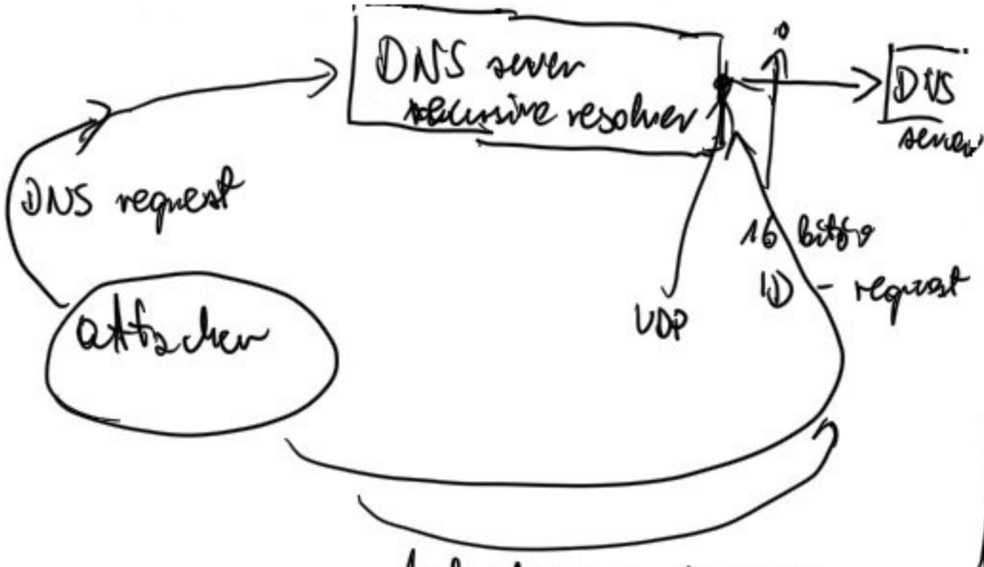
DNS - cache poisoning



If the attacker
will correctly guess the address
of the requested DNS server,
UDP port, and ID of request

and will be quicker
than the genuine server then
the cache will be poison.

DNS Sec

First version in 1997.

DNS Sec introduces PKI into DNS
and signatures that authenticate
Resource Records.

So DNS Sec adds a few
new DNS record types:

RRSig - for signatures

DNSKey - contains public
key for signature
verification

DS - Contains a hash of a DNSKey
record.

NSEC and NSEC3 - denial of existence
of a DNS record.

DNSKEY, CDS – they are used for child zone updates.

First step is to group Resource Records having the same name and type

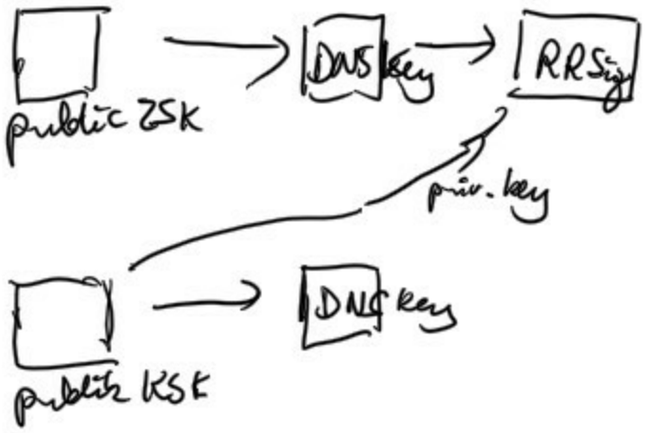
www.example.com	A	172.16.4.17
" "	A	172.16.4.20

So such resource records are grouped into sets (RRset) and one signed with ZSK (Zone Signing key).

To make the signature verifiable the zone operator also publishes ZSK in the DNSKey record.

How ZSK is authenticated?

The KSK is used for that purpose



KSK is used only for signing ZSKs, ZSK is used for signing everything else (RRsets)

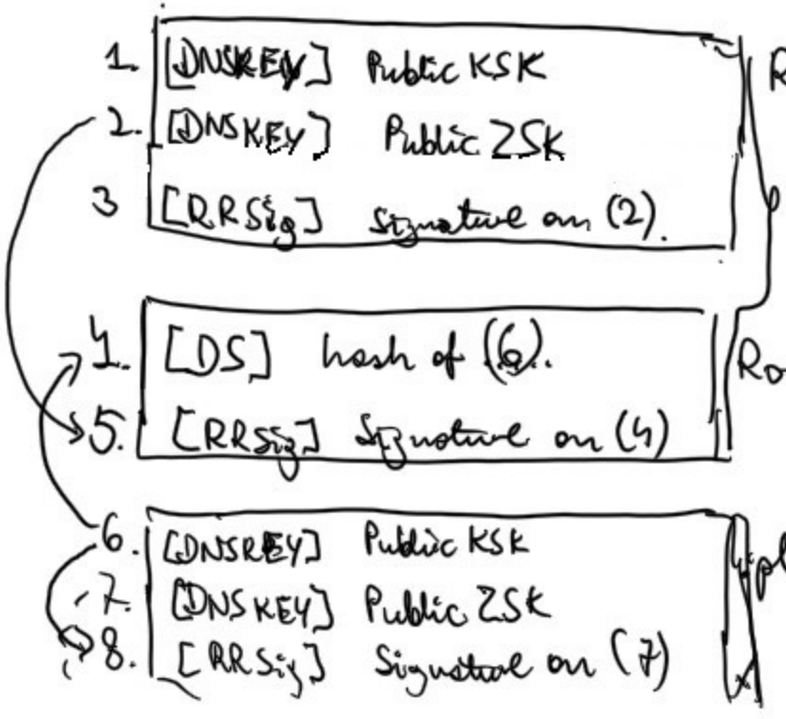
This distinction allows to make frequent changes of ZSK → KSK

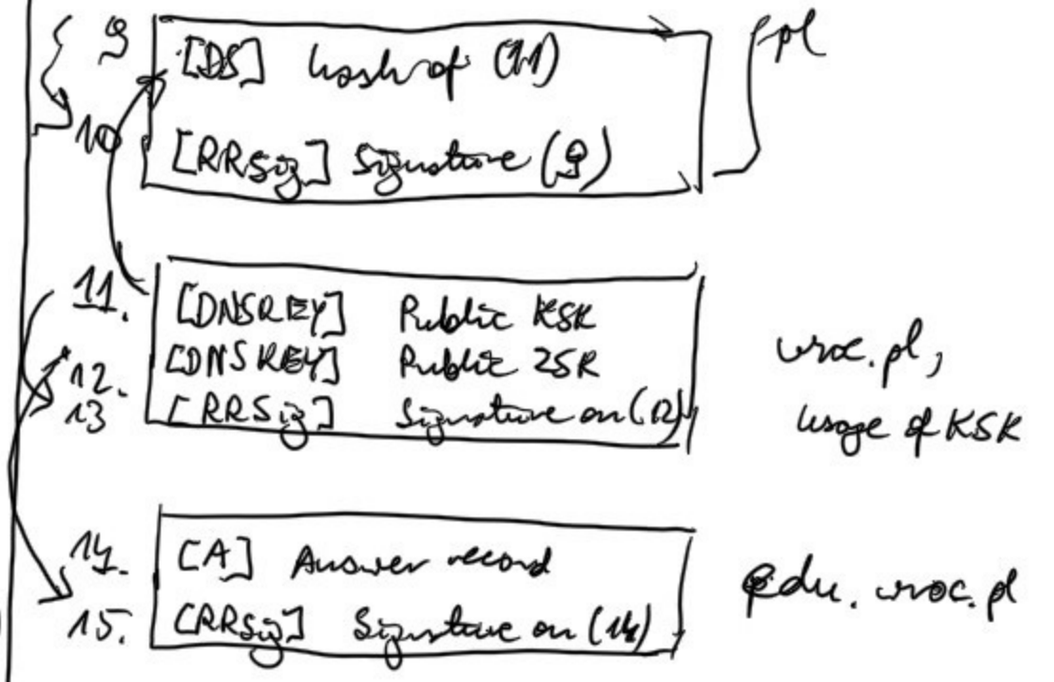
is linked to the parent ZONE:

DS record in the parent zone contains a hash of the RSK (see key tag - Sect. 5.1 of RFC 4034)

key value, name and algorithm

So we build a hierarchy.





NSEC - , NSEC3

(next secure) - a proof that there is no entry like e.g.:

a.a.priv.edu.wroc.pl

But this allows resource records enumeration:

priv.pwr.edu.wroc.pl

such a record can be returned by NSEC, but this subdomain is intended to remain private.

NSEC3 replaces NSEC and uses hashes.

Unfortunately, DNSSec is not widely deployed: in 2017 30% TLD and 47% country code TLDs (ccTLDs) were DNSSec enabled.

Moreover, there are some issues with resolvers:

if new unsupported algorithms are listed in signed DNS responses (even if a domain supports multiple algorithms and only some of which are unknown to the resolver) the resolvers do not validate DNSSec - this opens doors to cache poisoning attacks.