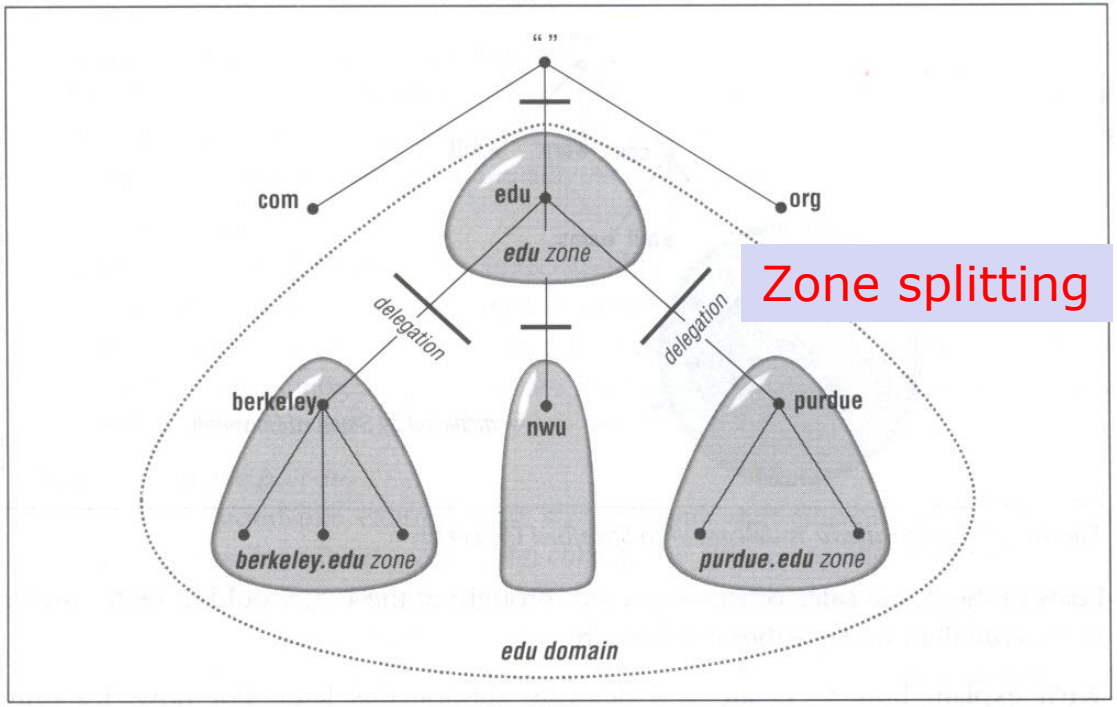
Chap. 8 (added) DNS Security

- DNS Service
- DNS Attacks
- DNSSEC (DNS Security)

DNS name service

- Domain: a subtree of a domain name space
- Zone: some part of the domain name space
  - Authoritative name servers have complete information about a zone
- Distributed management thru delegation



DNS name servers

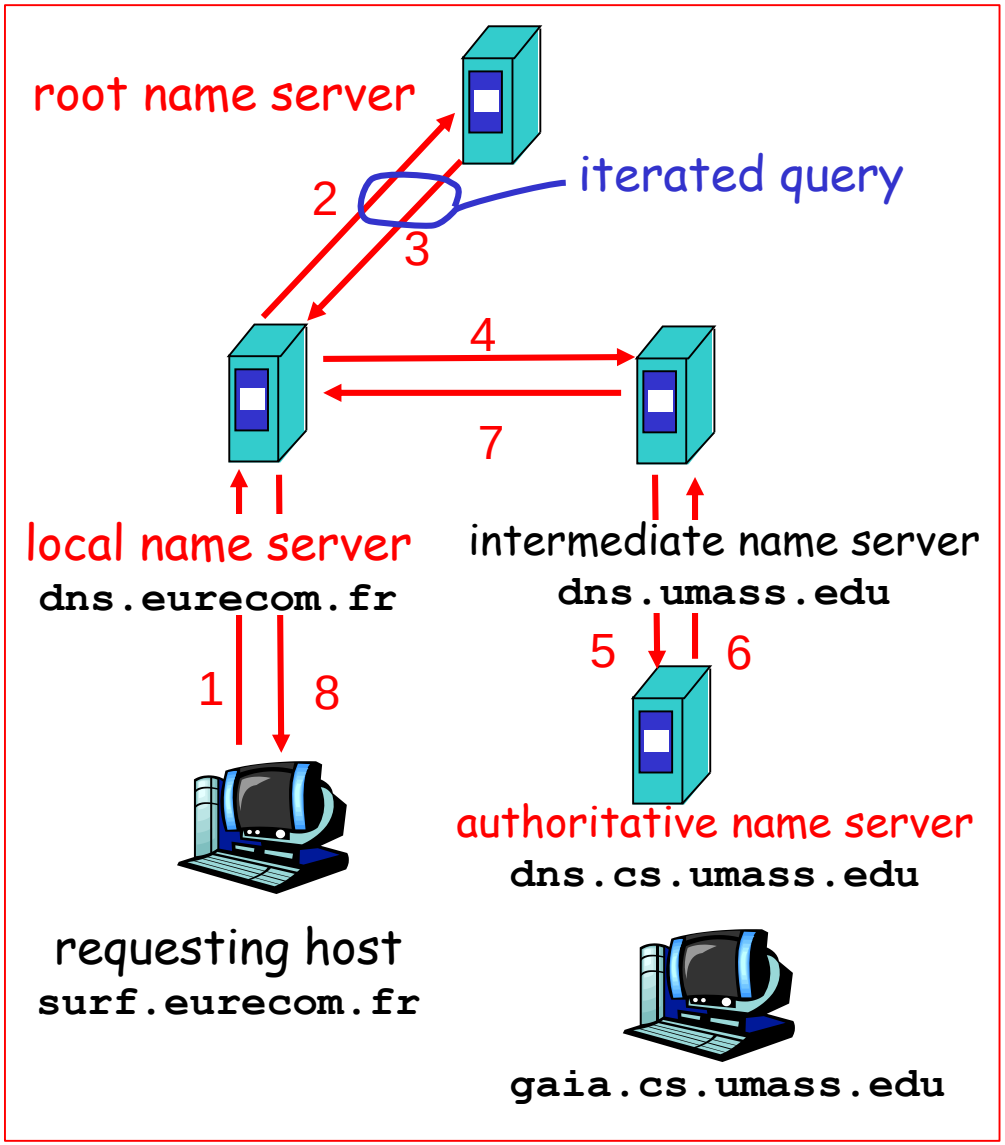
- Distributed database: no server has all name-to-IP address mappings
- local name servers:
  - each ISP, company has local (default) name server
  - host DNS query first goes to local name server
- authoritative name server:
  - keeps DNS info. for hosts within a specific zone
  - can perform name/address translation for that host's name

DNS name servers

- root name server:
  - contacted by local name server that can not resolve name
  - contacts authoritative name server if name mapping not known
  - gets mapping
  - returns mapping to local name server
  - dozen root name servers worldwide

DNS: iterated queries

- Resolver:
  - queries the name server
  - interpret the responses
  - return result to user
- recursive query:
  - puts burden of name resolution on contacted name server
- iterated query:
  - contacted server replies with name of server to contact



DNS: caching records

- DNS caching
  - Once name server learns mapping, it caches mapping
  - cache entries timeout (disappear) after some time

DNS Resource Records

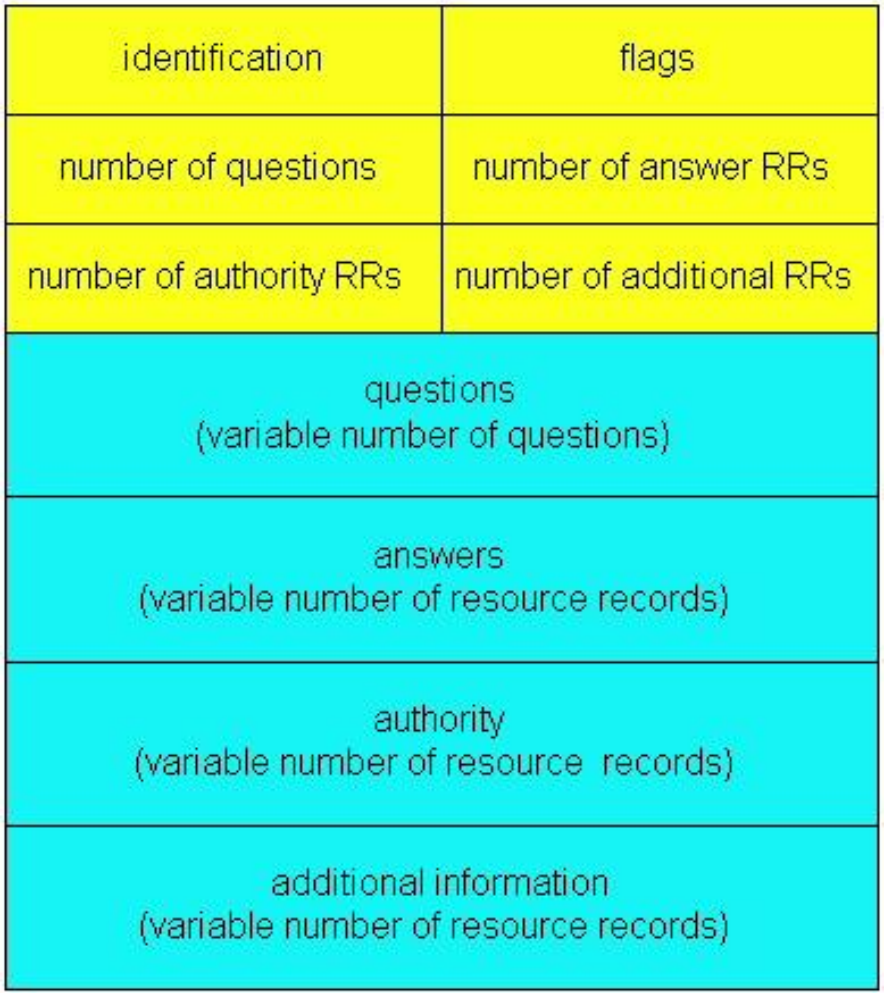
- DNS: distributed DB storing resource records (RR)

RR format: `(name, value, type,ttl)`

- Type=A
  - name is hostname
  - value is IP address
- Type=NS
  - name is domain
  - value: IP addr of authoritative name server for this domain
- Type=CNAME
  - name is an alias name for some "canonical" name
  - value is canonical name
- Type=MX
  - value is hostname of mail-server associated with a name (domain name)

DNS protocol, messages

- DNS protocol : query and reply messages, both with same message format
- msg header
  - identification: 16 bit # to match query and reply
  - flags:
    - query or reply
    - recursion desired
    - recursion available
    - reply is authoritative



DNS query

- Troubleshooting tools for DNS
  - nslookup
  - dig (domain information gopher)

```
$ dig cic.ulsan.ac.kr          ; looks up A records for
                               ; cic.ulsan.ac.kr

$ dig ulsan.ac.kr mx

                               ; looks up MX records for
                               ; ulsan.ac.kr

$ dig @a.root-servers.net  .  ns

                    ; queries a.root-servers.net (name server)
                    ; for NS records for  .  domain
```

DNS query

```
gslacks[pts/3]:~> dig www.cse.ucsc.edu
; <<>> DiG 8.2 <<>> www.cse.ucsc.edu
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: RESPONSE, status: NOERROR, id: 4
;; flags: aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      www.cse.ucsc.edu, type = A, class = IN
;; ANSWER SECTION:
www.cse.ucsc.edu.       1D IN CNAME     ftp.cse.ucsc.edu.
ftp.cse.ucsc.edu.       1D IN A         128.114.48.173
;; AUTHORITY SECTION:
cse.ucsc.edu.           1D IN NS        services.cse.ucsc.edu.
cse.ucsc.edu.           1D IN NS        fs1.cse.ucsc.edu.
;; ADDITIONAL SECTION:
services.cse.ucsc.edu.  1D IN A         128.114.48.10
fs1.cse.ucsc.edu.       1D IN A         128.114.48.11
.....
```

qr: query packet
aa: authoritative answer
rd: recursion desired
ra: recursion available

DNS query

```
gslacks[pts/3]:~> dig www.cse.ucsc.edu
; <<>> DiG 8.2 <<>> www.cse.ucsc.edu
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: RESPONSE, status: NOERROR, id: 4
;; flags: rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      www.cse.ucsc.edu, type = A, class = IN
;; ANSWER SECTION:
www.cse.ucsc.edu.       23h59m57s IN CNAME  ftp.cse.ucsc.edu.
ftp.cse.ucsc.edu.       23h59m57s IN A  128.114.48.173
;; AUTHORITY SECTION:
cse.ucsc.edu.           15h54m19s IN NS  services.cse.ucsc.edu.
cse.ucsc.edu.           15h54m19s IN NS  fs1.cse.ucsc.edu.
;; ADDITIONAL SECTION:
services.cse.ucsc.edu.  15h54m19s IN A  128.114.48.10
fs1.cse.ucsc.edu.       15h54m19s IN A  128.114.48.11
```

.....

Zone transfer

- Name servers for a zone
  - Primary (master) name server: reads zone data from a file on its host
  - Secondary (slave) name server: gets zone data from primary name server that is authoritative for the zone
- Zone transfer:
  - When a slave name server starts up, it contacts its master server and pulls the zone data over

```
$ dig @192.168.1.85 dumb.target.net  axfr
                        ; transfer zone dumb.target.net from 192.168.1.85
```

DNS Package: BIND

- DNS package in unix: BIND
  - it has many security problem history
- DNS daemon in unix
  - a process called “named”
  - Configuration file: /etc/named.conf

DNS configuration: /etc/named.conf

```
// Config file for name server

options {
        directory "/var/named";
        version "bla bla bla"
        allow-transfer {192.154.1.30};
};

zone "." in {
        type hint;
        file "root.hints";
};

zone "foobar.brian.edu" in {
        type master
        file "pz/db.foobar.brian.edu"

zone "1.154.192.in-addr.arpa" in {
        type master;
        file "pz/db.192.154.1";
};
```

zone file directory

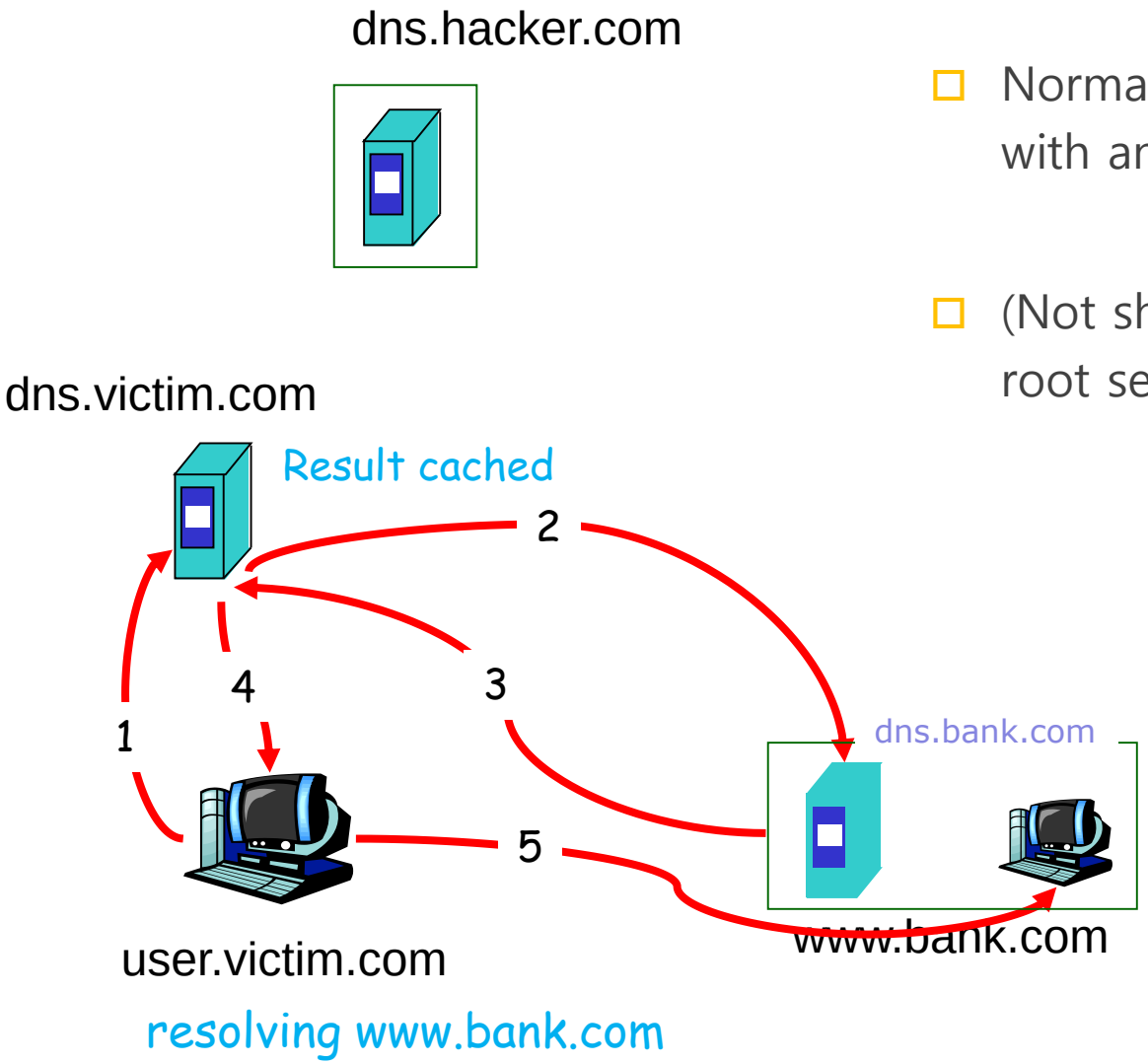
secondary name server

contains name and IP address of root name server

For converting from name to address

For converting from address to name

DNS Operation – Normal

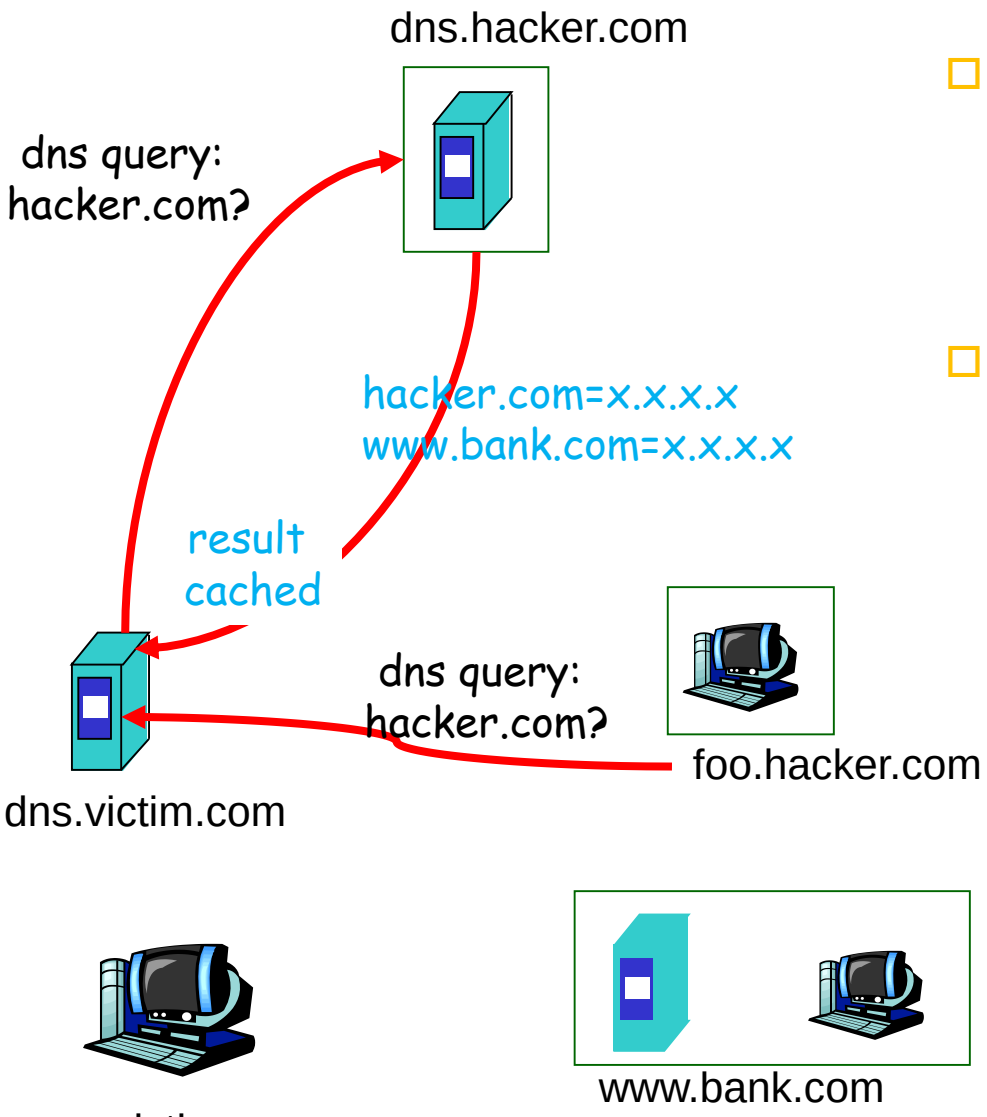


- Normally, DNS is resolved with an authoritative server
- (Not shown is lookup to .com root server)

DNS Cache Poisoning

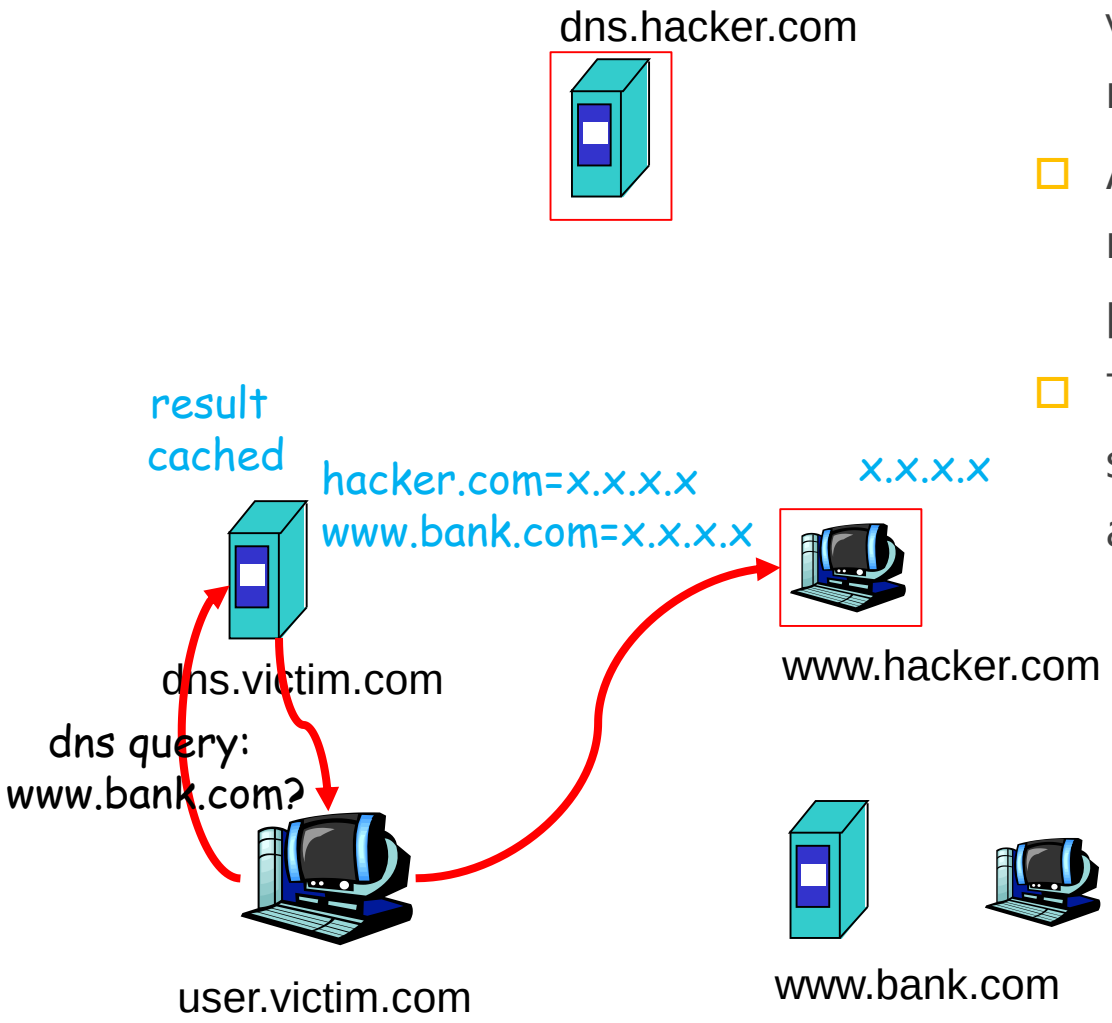
- URL spoofing attack:
  - register a similar name of someone you are attacking
  - e.g., www.ibn.com, …
- Cache poisoning is a more sophisticated version of the same idea
- The two key ideas for the attack are:
  - The query number (and reply id) are often predictable if you can learn earlier IDs
  - DNS caches previous results

Old Version of the Attack



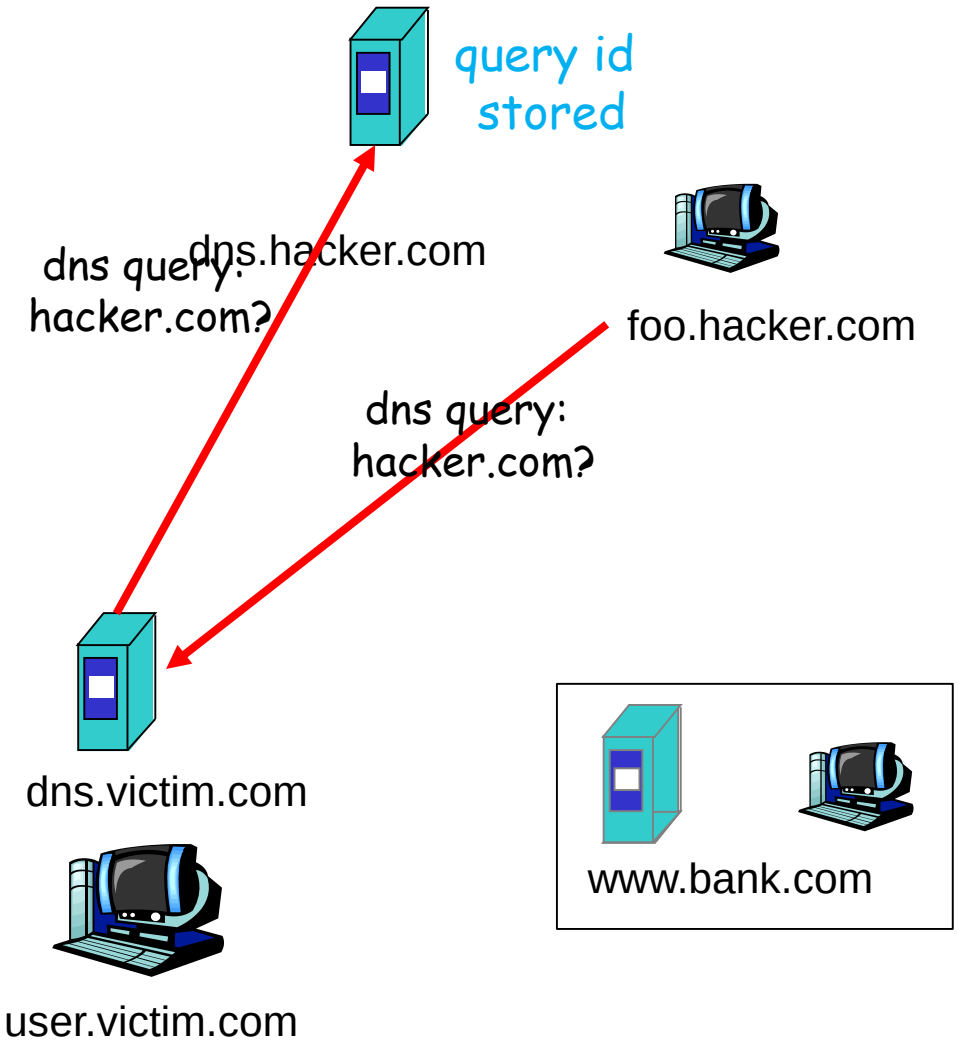
- On older versions of BIND, replies that came in could include additional lookup information (additional info section)
- This additional lookup information would be stored for future use

Old Version of the Attack



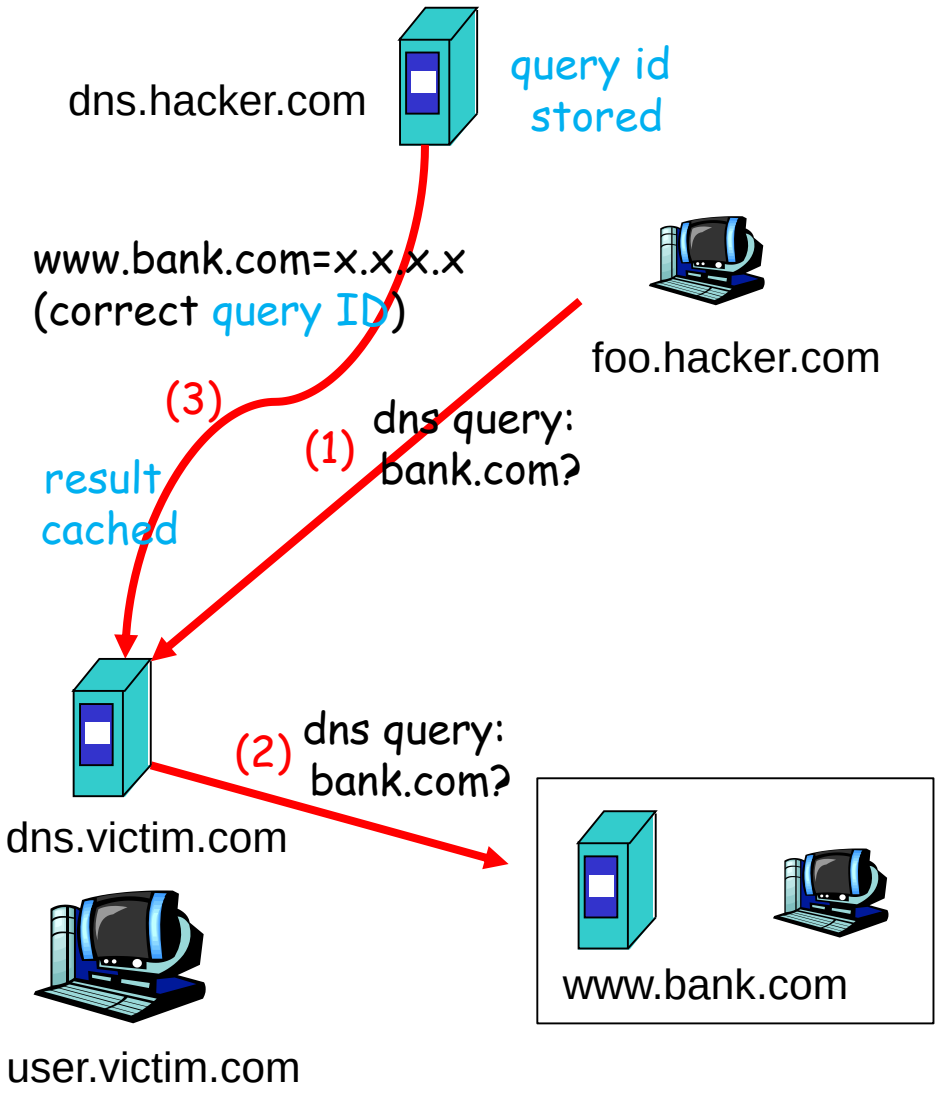
- The next time a user from victim.com looks for the bank, is redirected to the hacker's site
- All the hacker has to do is create a mock-up of the banks site to get passwords, etc.
- The old attack no longer work since BIND was patched to ignore additional information

The Attack - more



- The first step of the attack is to learn victim.com's current query id number
- The simplest way to do that is to get the victim to query the attacker's DNS machine
- This querying can be repeated many times to know how the query ids change over time

The Attack - more



- Early versions of DNS servers deterministically incremented the ID field; it was patched by random query IDs
- Birthday attack
  - 16-bit query ID (only 65,536 options)
  - the resolver sends many queries, with different IDs, at the same time
  - Send hundreds of reply with random transaction IDs at the same time
  - Increase the probability of making a correct guess

Defenses

- New versions of BIND have harder to predict query IDs
- DNSSEC : RFC 2535
  - a secure version of DNS with RSA signed DNS records
- Authentication of DNS responses
  - Each DNS response has a signature of the requested RR
  - Resolver authenticates response using the public key of the authoritative name server

Defenses

- Split-split defense:
  - One DNS server for resolving names for users inside your domain; this server doesn't respond to outside queries
  - Another separate DNS server is setup for responding to queries from outsiders
  - The two never exchange information
  - Your users are not subject to poisoned information

Defenses in /etc/named.conf

```
// name server config file
options {
        directory "/var/named";
        version "version bla bla"
        allow-transfer {192.154.1.30};
        allow-query { any; };
        allow-recursion { 192.154.1.0/24; };
};
zone "foobar.brian.edu" in {
        type master
        file "pz/db.foobar.brian.edu"
        allow-query { 192.154.1.0/24; }
};
zone "1.154.192.in-addr.arpa" in {
        type master;
        file "pz/db.192.154.1";
        allow-query { 192.154.1.0/24; }
};
```

Global access control list (ACL): Only this subnet can query us

Zone specific ACL: take precedence over a global ACL

Homework #3

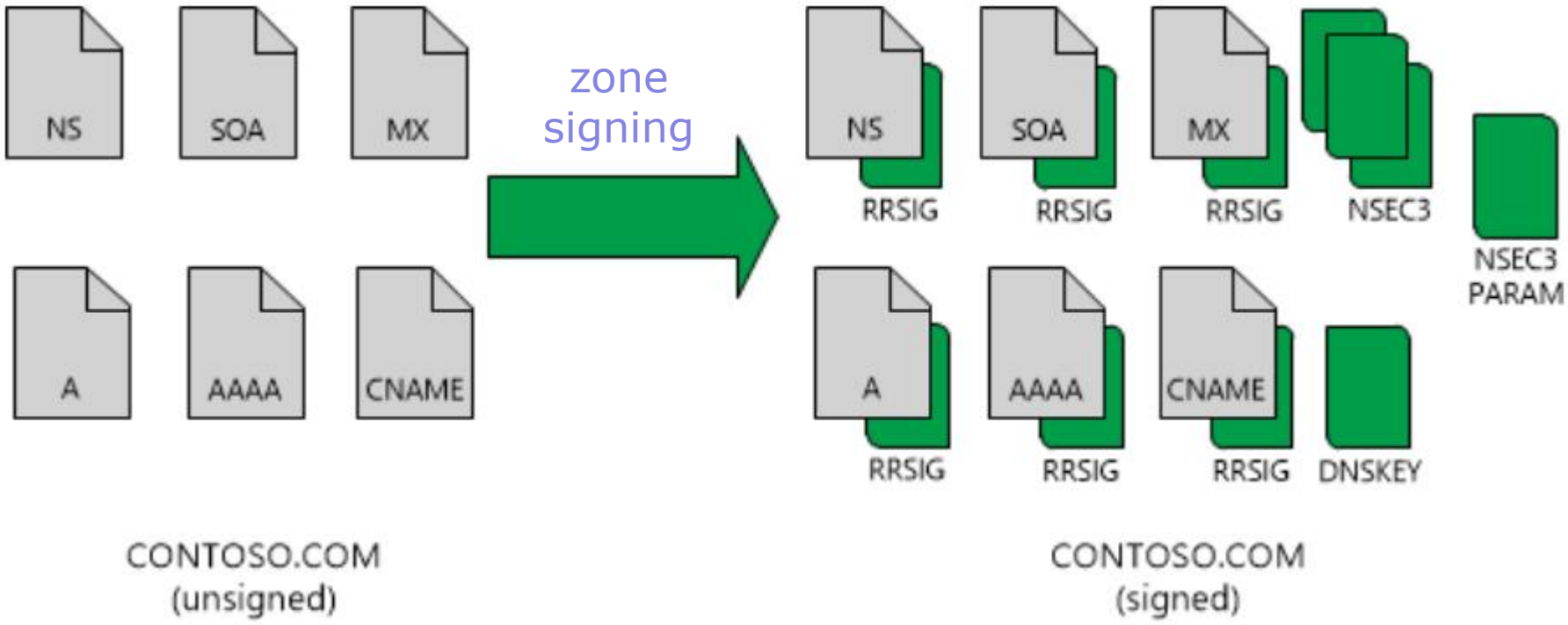
- BIND package 기능 조사:
  - BIND package 기능
  - /etc/named.conf 설정파일 기능
  - 호스트에서 name resolution 하는 과정: OS별(windows, linux) 조사
  - 파일 제출: “hw3-학번-이름.hwp”

DNSSEC (DNS Security)

- DNSSEC:
  - Security extension of DNS service
  - Authoritative name servers secure their zones by performing zone signing
  - provides end-to-end authentication using digital signatures b/w a resolver and an authoritative server
  - defines a set of new resource record types and modifications to the existing DNS protocol
  - RFC 4033, 4034, 4035

DNSSEC (DNS Security)

- DNSSEC:



DNSSEC (DNS Security)

- DNSSEC:
  - each DNSSEC-enabled authoritative NS can have two public keys
  - ZSK (Zone Signing Key):
    - used to sign the RRset of the Zone
  - KSK (Key Signing Key):
    - used to sign DNSKEY RRs
    - can be used as a trust anchor

DNSSEC (DNS Security)

DNSSEC Resource Records:

- DNSKEY resource record: defines the public key

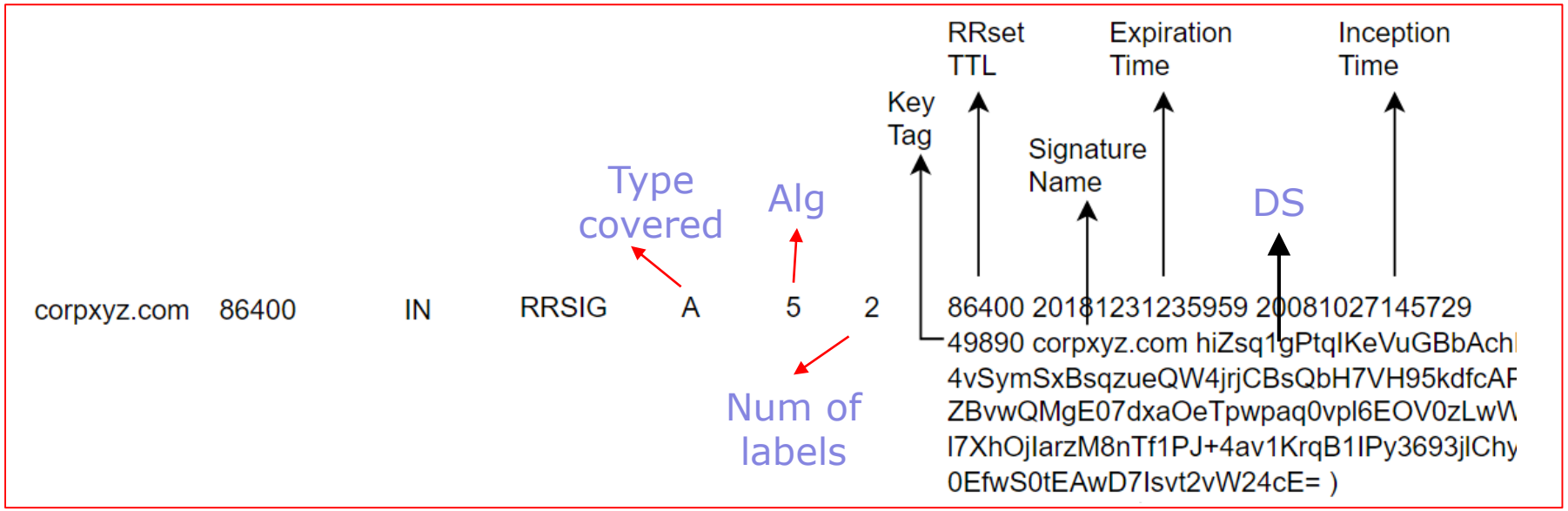
						Alg	Public key
corpxyz.com	1296000	IN	DNSKEY	257	3	5	20181231235959hiZsq1gPtq 4vSymSxBsqzueQW4jrjCBsC ZBvwQMgE07dxaOeTpwpaq I7XhOjlarzM8nTf1PJ+4av1Kr 0EfwS0tEAwD7Isvt2vW24cE
domain name	TTL	Class	Type	Flags	Proto		

Flags: DNSKEY-flag(bit7), KEY-type(bit15: ZSK or KSK);
256 (ZSK), 257 (KSK)
Proto: DNSSEC protocol type (3)
Alg: type of the public key algorithm
(RSA/MD5, DSA, RSA/SHA1, etc.)

DNSSEC (DNS Security)

DNSSEC Resource Records:

- RRSIG resource record: defines the signature of an RRset



Type covered: RR type covered by the RRSIG record
Alg: cryptographic algorithm used to create the DS (RSA/MD5, RSA/SHA-1, …)
Num of labels: the number of labels in the owner name of the signed records
Key tag: key tag value of the DNSKEY RR that validates the signature
RRset TTL: TTL value of the RRset covered by the RRSIG record
DS: Base64 encoding of the digital signature

DNSSEC (DNS Security)

DNSSEC Resource Records:

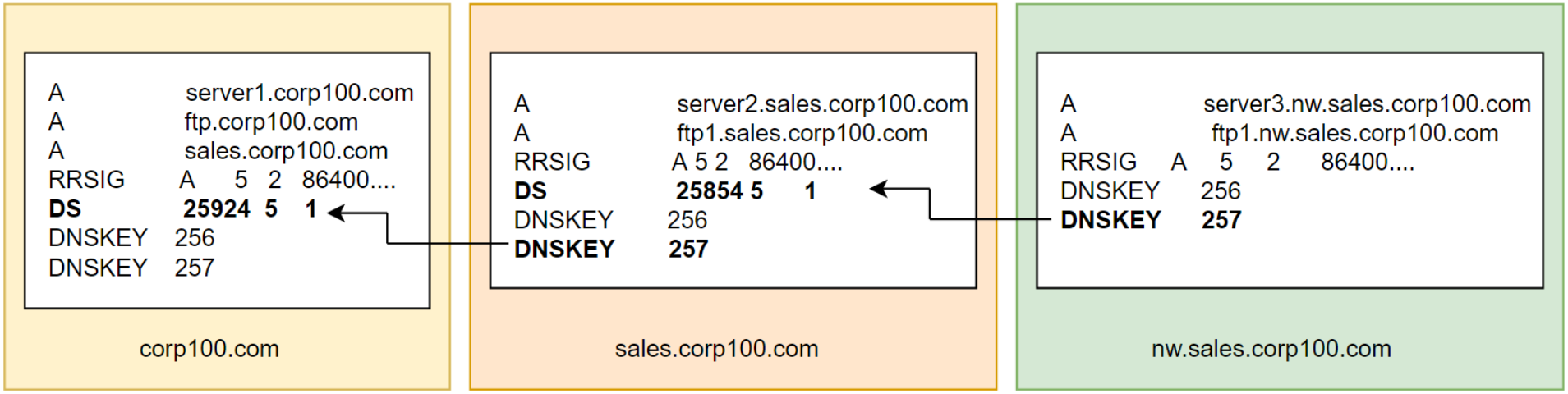
- DS (Delegation Signer) resource record:
  - contains a hash of a child zone's KSK and can be used as a trust anchor
  - creates a secure delegation point for a signed subzone

corpxyz.com	86400	IN	DS	25924	5	1	49D2801B B622B1F8
				Key tag	Alg	Digest type	Digest value

Key tag: key tag value of the DNSKEY RR to which this DS RR refers
Alg: the algorithm of the DNSKEY RR to which this DS RR refers
Digest type: algorithm used to create the digest; 1 (SHA-1), 2 (SHA-256)
Digest : digest value of the DNSKEY RR to which this DS RR refers

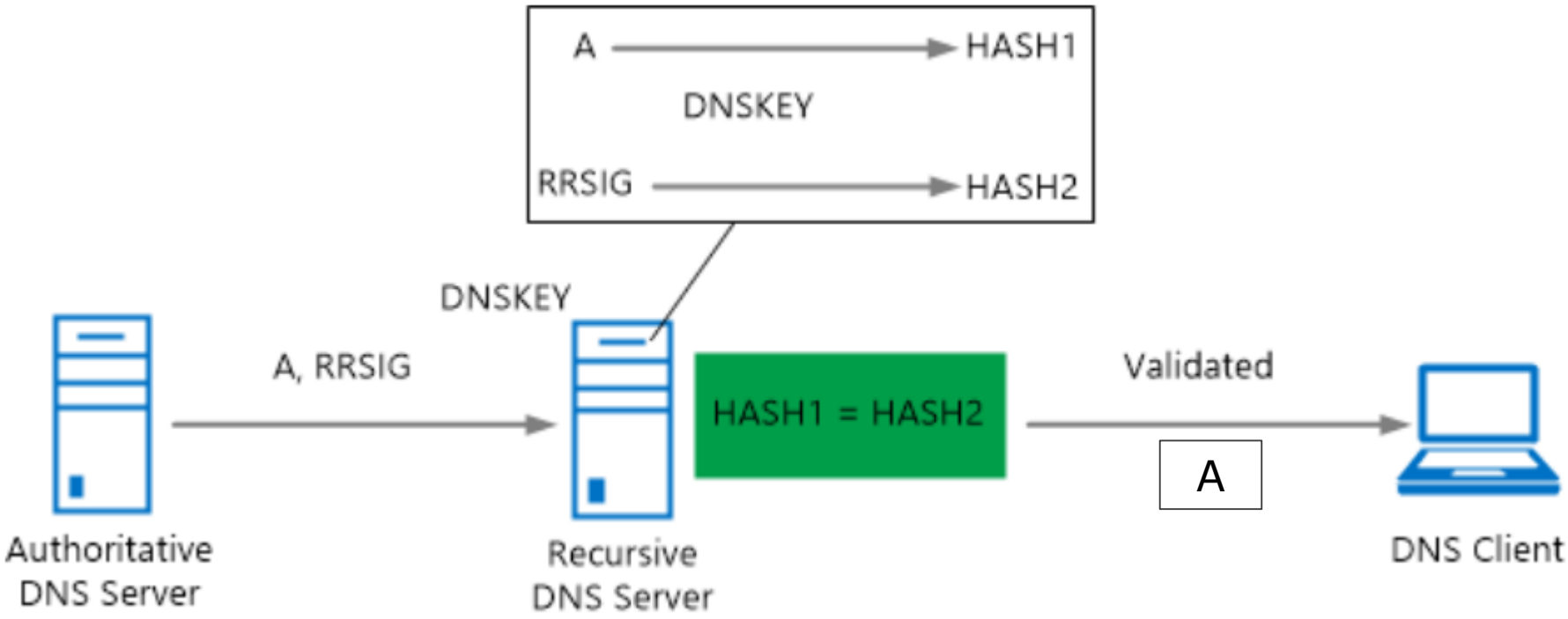
DNSSEC (DNS Security)

- DNSSEC Resource Records:
  - a chain of trust thru DS (Delegation Signer) resource record



DNSSEC (DNS Security)

- Validation process:
  - A DNS server receives RRset and DNSKEY, RRSIG RRs
  - uses the DNSKEY RR to validate responses from the authoritative DNS server by decrypting digital signatures



DNSSEC (DNS Security)

- Zone signing process: