DNS and DNSSEC

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Security of IT infrastructure (2023/24)

Content

DNS (Domain Name System)

- hierarchical, distributed, decentralized system
- maps domain names to IP addresses and vice versa
- tree structure (zones, delegation of responsibilities)
- 13 root “servers” (a, b, …, m) – clusters
  - operated by 12 independent organisations
  - Anycast routing
- examples (April 2024, www.root-servers.org):
  - “c” (operated by Cogent Communications) has 12 sites, 1 in Bratislava
  - “f” (operated by Internet Systems Consortium) has 345 sites, 1 in Bratislava
  - “i” (operated by Netnod) has 81 sites, 1 in Bratislava
  - “j” (operated by Verisign) has 150 sites, 1 in Bratislava
  - “l” (operated by ICANN) has 132 sites, 1 in Bratislava

DNS – Resource records

- client – server architecture
- resource record types (RR – resource record):

SOA	start of authority
A	address (IPv4)
AAAA	IPv6 address
NS	name server
MX	mail exchange
CNAME	canonical name (alias)
PTR	pointer record ...

DNS – components

- DNS servers:
  - authoritative – for own zone and for nameservers of delegated subzones
  - recursive – query other DNS servers to answer client requests
    … + caching functionality – remembering resolved records (efficiency)
- DNS resolvers (clients)
  - part of an operating system or application
  - usually include caching functionality
- Protocol:
  - UDP, port 53
  - stateless (query – response)
  - no confidentiality, integrity or authenticity features
  - now: TCP used as well
  - RFC 7766 (2016) DNS Transport over TCP – Implementation Requirements
    All general-purpose DNS implementations MUST support both UDP and TCP transport.

Some security-related applications employing DNS

- proof of domain ownership
  - Let's Encrypt: DNS challenge (TXT record) as an option
  - Office 365 (TXT record)
- DANE (DNS-based Authentication of Named Entities)
  - binding X.509 (TLS) certificates to names in DNS (even without CA)
  - TLSA resource record, signed by DNSSEC
  - can be used for SMTP (e.g., see Microsoft Exchange Online)
- DNS Certification Authority Authorization (RFC 6844)
  - CAA record specifies Certification Authorities which are allowed to issue certificates for the domain
  - adoption rate (SSL Pulse, https://www.ssllabs.com/ssl-pulse/): 8.3% (II/2021), 12.2% (I/2022), 13.4% (II/2023), 15.0% (IV/2024)
- SPF (Sender Policy Framework)
  - (TXT record) what SMTP servers are authorized to send mail

Some security issues

Authenticity and integrity

- DNS spoofing / cache poisoning (client, mail server etc. redirected to fake IP address)
  - attacker answers to client before his (recursive) DNS server
  - attacker answers to DNS server before the authoritative DNS server
  - attacker changes the response of the DNS server
  - attacker inserts additional information (e.g. NS records) about other zone into his zone's response, ...
  - long TTL for fake IP addresses
- some ideas how to make spoofing harder:
  - RFC 5452 Measures for Making DNS More Resilient against Forged Answers
- weaknesses in protocol design, issues in DNS server implementations (e.g., vulnerabilities in bind (NVD): 2021/6, 2022/11, 2023/9)

DoS

- DNS amplification attack
  - DNS server's responses can be much longer than the queries
  - source IP address spoofing
  - publicly open DNS servers … DDoS attack
  - counting open resolvers (https://scan.shadowserver.org/):
    $\sim$ 1.95 mil. IPv4, 0.52 mil. IPv6 (IV/2024)
- possible mitigations of amplification attack:
  - Disabling Recursion on Authoritative Name Servers
  - Limiting Recursion to Authorized Clients
  - Response Rate Limiting

DNS in applications

- DNS rebinding
  - target the same-origin policy in a web browser
  - the first response of attacker's DNS server with short TTL
  - web browser loads malicious code
  - following query is answered by sending internal IP address
  - …attacking internal web
- mitigation of DNS rebinding:
  - DNS pinning – locking IP address to value from the first DNS response
  - filter out the private IP addresses from DNS responses, etc.
- Threat Analysis of the Domain Name System (DNS), RFC 3833
- DNS cookies (RFC 7873)

  "limited protection to DNS servers and clients against a variety of increasingly common denial-of-service and amplification/ forgery or cache poisoning attacks by off-path attackers"

Malware, C&C, tunneling

- attacker owns an authoritative DNS server
  - any DNS request by victim reaches DNS server
  - any response reaches the victim
- commands and data transfer via DNS
  - malware
  - firewall bypassing
  - captive portal avoidance
- DNS protocol often unmonitored
  - DNS traffic analysis
  - unusual data, number of request, DNS server location, etc.

DNS – some cryptographic solutions to security problems

- TSIG
  - Transaction Signatures (RFC 2845)
  - HMAC-MD5 and shared secrets for authentication
  - primary use for dynamic updates of DNS records, zone transfers etc.
  - no means how to manage/distribute shared secrets
- SIG(0)
  - DNS Request and Transaction Signatures (SIG(0)s), RFC 2931
  - digital signatures for dynamic DNS updates
  - public key part of the zone
- DNSSEC
  - *today's focus …*

DNSSEC – introduction

- Domain Name System SECurity extensions

RFC 4033	DNS Security Introduction and Requirements
RFC 4034	Resource Records for the DNS Security Extensions
RFC 4035	Protocol Modifications for the DNS Security Extensions
RFC 5011	Automated Updates of DNSSEC Trust Anchors
RFC 5155	DNSSEC Hashed Authenticated Denial of Existence
RFC 6840	Clarifications and Implementation Notes for DNSSEC
…	

- Main idea: digitally signed DNS records (by DNS server)

  …DNSSEC itself is concerned with object security of DNS data, not channel security of DNS transactions.

- Goals:
  - data authenticity and integrity
  - authenticity of non-existent data

DNSSEC does not provide

- data confidentiality (no encryption)
  - no solution to privacy issues
- DoS attacks protection
  - for DNS server
  - for clients (DNS amplification)
  - DNSSEC can worsen the situation – signature verification, longer responses

Current state (1)

https://ithi.research.icann.org/

- July 2010: DNS root zone signed
- February 2020: (1516 TLDs in the root zone / 1389 signed)
- April 2024:
  - 92.68% of Top Level Domain zones signed
  - 63.71% of Country Code Top Level Domain zones signed

Current state (2)

- sk. TLD:
  - official start of DNSSEC in April 2019
  - try: `dig @8.8.8.8 sk DS +dnssec`
    or `dig @a.tld.sk sk DNSKEY +dnssec`
- com. zone signed in March 2011
  - current state – negligible DNSSEC deployment in 2nd level domains
  - approx. 4.3% of domains in com. signed (www.statdns.com, IV/2024)
  - nothing: google.com, meta.com, microsoft.com, apple.com …
- Google Public DNS servers (8.8.8.8, 8.8.4.4) support DNSSEC validation by default since 2013

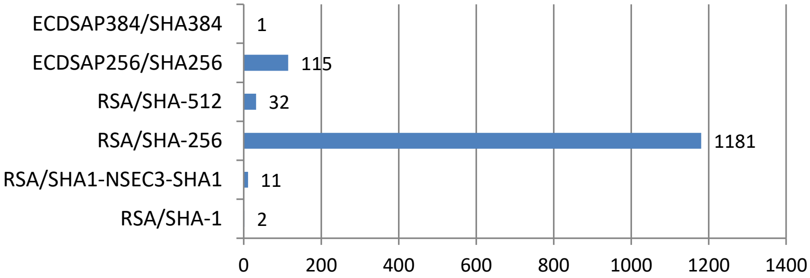
Keys a algorithms

- Key Signing Keys (KSK)
  - signing other keys in DNSKEY records
  - DS record needs to be published in parent zone (public key fingerprint)
- Zone Signing Keys (ZSK)
  - signing other records in the zone
  - simple management of ZSK (completely managed by the zone)

- the most frequent algorithms: RSA (usually 2048 bits) with SHA-256
  - digital signature scheme: RSASSA-PKCS1-v1.5 (PKCS #1)
  - RSA key length max. 4096 bits
    (min. 1024 for RSA/SHA-512, 512 for RSA/SHA-256)

Algorithms – root zone

- DS records in the root zone (IV/2024):



A recent vulnerability in DNSSEC

- E. Heftrig et al., *Downgrading DNSSEC: How to Exploit Crypto Agility for Hijacking Signed Zones*, USENIX 2023
- cryptographic agility – new algorithm deployed in DNSSEC
- How should the resolvers react to records signed with unknown algorithms?
- lack of clear specification
- result: downgrade attacks, cache poisoning
- 2021 – 65% of open resolvers vulnerable (including public DNS servers by Google and Cloudflare)
- 2022 – reduced to 7.5%

New DNS record types – DNSKEY and DS

examples from the root zone

`http://www.internic.net/zones/root.zone`

- DNSKEY – public key

```
.   172800 IN DNSKEY 256 3 8 AwEAAZBALoO...I0=
.   172800 IN DNSKEY 257 3 8 AwEAAaz/tAm...bU=
```

  - . 172800 IN – owner, TTL, class
  - 256, 257 – flags (256: ZSK; 257: KSK, the last bit denotes SEP (Secure Entry Point))
  - 3 – protocol (fixed)
  - 8 – algorithm (RSA/SHA-256)
- DS (Delegation signer) – KSK identification (for delegated zone)

```
sk.   86400 IN DS 2324 13 2 3E7E4F60EC...205
```

  - 2324 – key tag (for fast selection of DNSKEY record)
  - 13 – algorithm corresponding to referenced DNSKEY record (ECDSA P-256 with SHA-256)
  - 2 – hash function (SHA-256) used for digest calculation

New DNS record types – DNSKEY and DS

examples from the root zone

`http://www.internic.net/zones/root.zone`

- DNSKEY – public key
  ```
  .   172800 IN DNSKEY 256 3 8 AwEAAZBALoO...I0=
  .   172800 IN DNSKEY 257 3 8 AwEAAaz/tAm...bU=
  ```
  - . 172800 IN – owner, TTL, class
  - 256, 257 – flags (256: ZSK; 257: KSK, the last bit denotes SEP (Secure Entry Point))
  - 3 – protocol (fixed)
  - 8 – algorithm (RSA/SHA-256)
- DS (Delegation signer) – KSK identification (for delegated zone)
  ```
  sk.  86400 IN DS 2324 13 2 3E7E4F60EC...205
  ```
  - 2324 – key tag (for fast selection of DNSKEY record)
  - 13 – algorithm corresponding to referenced DNSKEY record (ECDSA P-256 with SHA-256)
  - 2 – hash function (SHA-256) used for digest calculation

Root zone

- Management of KSK and ZSK for the root zone:
  - DNSSEC Practice Statement for the Root Zone KSK Operator
  - DNSSEC Practice Statement for the Root Zone ZSK Operator
- ZSK rollover: quarterly (ceremony – video, script, audit logs, ...)
- Publishing KSK:
  - DNSSEC Trust Anchor and Keys Publication for the Root Zone
  - XML (digest), p7s (S/MIME signature), pem (certificates for validating the signature)
  - available via HTTPS: `https://www.iana.org/dnssec/files`
  - 2016: new KSK generated (KSK-2017)
  - the root zone contains KSK-2017
  - KSK rollover postponed and then performed successfully in October 2018 (1 year later than planned)
  - KSK-2010 revoked in January 2019
  - KSK-2023 was planned, suspended (HSM vendor problem)
  - KSK-2024 should be generated on 26 April 2024

New DNS record types – RRSIG

- RRSIG – signature for a record set

  `sk. 86400 IN RRSIG DS 8 1 86400 20240430170000 20240417160000 5613 . D+8K6...Lw==`

  - `sk. 86400 IN RRSIG` – owner, TTL, class, type
  - DS – type that the signature covers
  - 8 – signing algorithm (RSA/SHA-256)
  - 1 – the number of labels (used to validate $*$)
  - 86400 – original TTL value
  - 20240430170000 20240417160000 – signature validity (until 30.04.2024 17:00 UTC, starting 17.04.2024 16:00 UTC) ~ 13 days
  - 5613 – key tag of the key in DNSKEY record for signature verification
  - . – singer's name (the owner in the DNSKEY record)
  - and finally, the signature

RRSIG

- a record set is signed (RRset)
  - RRset is determined by shared attributes: owner, class, type
- some records are unsigned:
  - NS records of delegated zones
  - A, AAAA records of delegated zones
  - these are data of delegated zones (not their parent zone)

Authenticated denial of existence – NSEC

- How to answer that a record does not exist?
- we don't want to sign on-line (access to private key required, slow)
- sorted records (canonical order)
- NSEC – "next secure" record

```
cz.  86400 IN NSEC dabur.  NS DS RRSIG NSEC
cz.  86400 IN RRSIG NSEC ...
```

  - for particular domain name (`cz.`)
  - `dabur.` – next owner (domain name) in zone file
  - NS DS RRSIG NSEC – types of existing records for current owner/name (`cz.`)
- the last NSEC refers to the beginning (next owner)
- there is one RRSIG record for each NSEC record

Nonexistent record – response types

- NXDOMAIN (nonexistent domain name, e.g. `da.`)

```
$dig @8.8.8.8 da.
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4649
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, .
```

- NOERROR & ANSWER: 0 (the name exists but not the name with given type)

```
$dig @8.8.8.8 nic.de. A +short
81.91.170.12
$dig @8.8.8.8 nic.de. AAAA +short
$
```

Nonexistence responses using NSEC

- NXDOMAIN: in response (in authority section) – NSEC record with RRSIG, proving the missing domain name:

  `cz.  86400 IN NSEC dabur.  NS DS RRSIG NSEC`

  - no name between `cz.` and `dabur.`
- NOERROR & ANSWER: 0: in response (in authority section) – NSEC record with RRSIG, proving the missing type for the domain name:

```
$dig @8.8.8.8 ye. DS +dnssec
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43223
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4,..
...
ye.    86400    IN    NSEC     yodobashi. NS RRSIG NSEC
ye.    86400    IN    RRSIG    NSEC 8 1 86400 20240430200000
       20240417190000 5613 . U70pHU5...4isuw==
...
```

NSEC vs. NSEC3

- zone walking (domain names enumeration)
- nonexistent name (NXDOMAIN) leaks neighbors “above” and “below”
- possibility to enumerate the zone (~ zone transfer via NSEC)
  - number of queries approx. linear with respect to the number of records
- problem for DNSSEC deployment …solution: NSEC3

NSEC3

- replacement of NSEC records; domain names replaced with fingerprints

```
$dig @8.8.8.8 cz. MX +dnssec
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20142
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 4 ..
...
6nu2...cul4.cz. 894 IN NSEC3 1 0 10 E71BD2086D590C64
                6NU3...Q9HB  NS SOA RRSIG DNSKEY NSEC3PARAM
...
```

- record-chain ordered according fingerprint values
- resolver computes name's fingerprint and finds the value between fingerprints in NSEC3 record
- in practice multiple NSEC3 and corresponding RRSIG records are returned (wildcards in the zone ...details in RFC 7129)

NSEC3 (2)

- NSEC3 parameters

```
6nu2...cul4.cz. 894 IN NSEC3 1 0 10 E71BD2086D590C64
                6NU3...Q9HB  NS SOA RRSIG DNSKEY NSEC3PARAM
```

  - 1 – hash function (SHA-1)
  - 0 – flags (1 for opt-out feature – not all names get NSEC3 and RRSIG ...details in RFC 7129, usefull for large zones, insecure delegation)
  - 10 – iteration count for fingerprint calculation
  - `E71BD2086D590C64` – salt
  - next name's fingerprint, record types for current owner
- off-line attack on fingerprints (the space of domain names is limited)

Differences DNSEC vs. PKI

- no certificates
- no validity interval for keys (but signatures have validity interval)
- keys managed by corresponding zone
- trusting a public key:
  - trusting KSK of the root zone (static import) → ZSK (.) → DS (in . for de.) → KSK (de.) → ZSK (de.) → DS (in de. for .bund.de.) → KSK (bund.de.) → ZSK (bund.de)
    …and then we can verify RRSIG of A record for www.bund.de
  - of course: … + caching

CDS and CDNSKEY

- regular change of cryptographic keys
- CDS/CDNSKEY records can help with management of DS records
  - Automating DNSSEC Delegation Trust Maintenance (RFC 7344)
  - Managing DS Records from the Parent via CDS/CDNSKEY (RFC 8078)
  - signaling desired DS state from the child zone to its parent