DNSSEC Extension by Using PKIX Certificates

IETF 116, Yokohama

Hyeonmin Lee, Taekyoung (Ted) Kwon

Seoul National University

Disclaimer

- Many slides are adapted from our group’s previous presentation
  - February 17th, 2023, OARC 40

- We support DNSSEC in its current standards
  - We’d like to offer another option to DNS operators

DNSSEC Deployment [1/2]

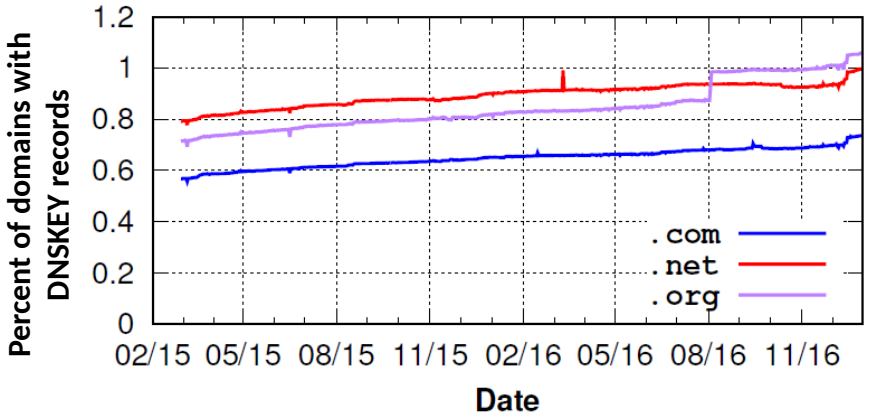
- DNS Security Extensions (DNSSEC) were introduced for integrity of DNS messages
- After two decades of DNSSEC introduction…

Top-level domains (TLDs)? 91% deployed DNSSEC[1]

Second-level domains (SLDs)?

- In Dec 2017[2] .com (0.75%)
  .net , .org (~1%)

- In Dec 2022[1] .com (3.6%)
  .net (4.2%)
  .org (4.8%)



DNSSEC deployment rate is still low..

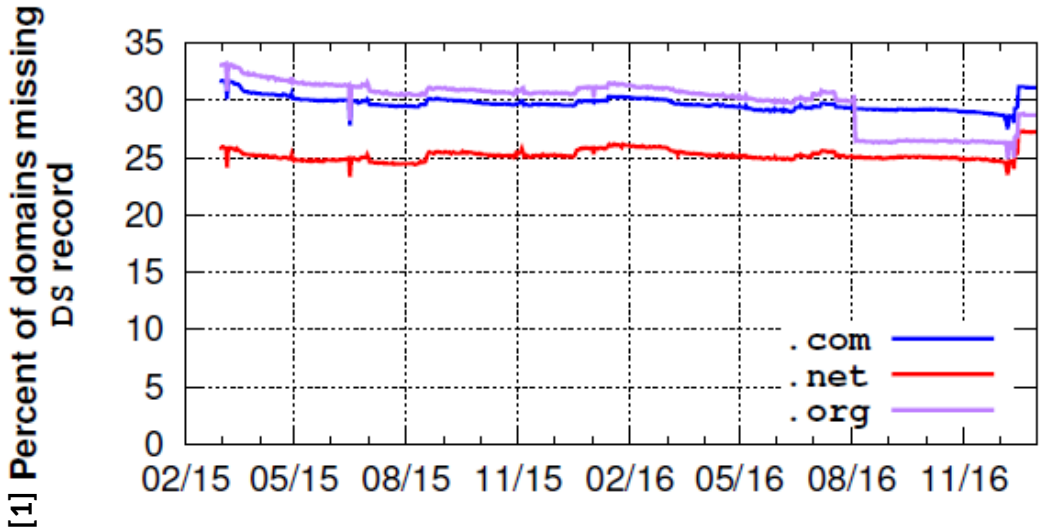
The vast majority of DNS messages in the real world are still vulnerable..

[1] dnssecstat (https://rick.eng.br/dnssecstat/) [2] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX Security'17)

DNSSEC Deployment [2/2]

- Deploying/managing DNSSEC is burdensome and complex..
  - To deploy DNSSEC, a domain has to publish three DNS records (DNSKEY, RRSIG, and DS) to establish a DNSSEC chain
  - **DS records have to be uploaded to the domain's parent zone**

- Errors in the DNSSEC deployment/management



30%

Missing DS records in the parent zone

[1] A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX Security'17)

Goal

- Can we guarantee the integrity of DNS messages without any dependency on other zones (e.g., uploading DS records to the parent zone)?

- We may need a more *easily deployable* way

It should **minimize changes or cooperations of** entities in the DNS infrastructure such as parent zones or registrars

Leveraging PKIX Certificates issued by CAs

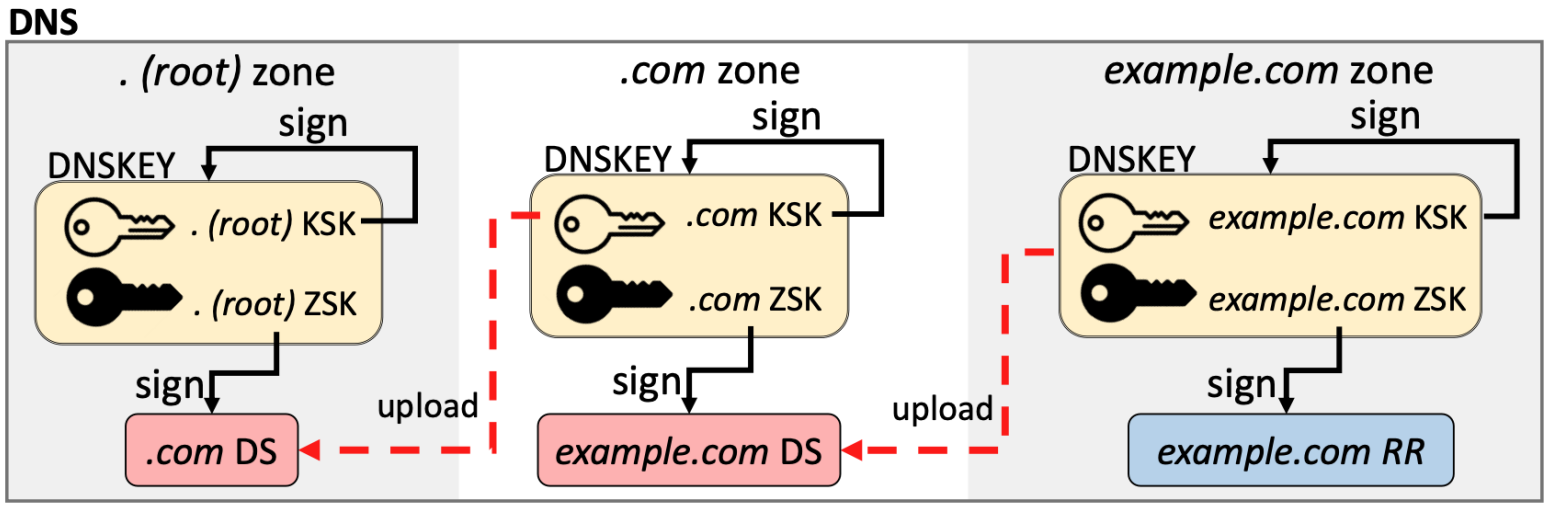
- Most domains already use public keys (in X.509 certificates) – for HTTPS/TLS
  - 94% of web traffic to Google is HTTPS [3]
  - Usually, certificates are issued by public CAs – the issuance process is well established and often automated (e.g., IETF ACME)

We can leverage PKIX certificates that have been successfully used by HTTPS/TLS

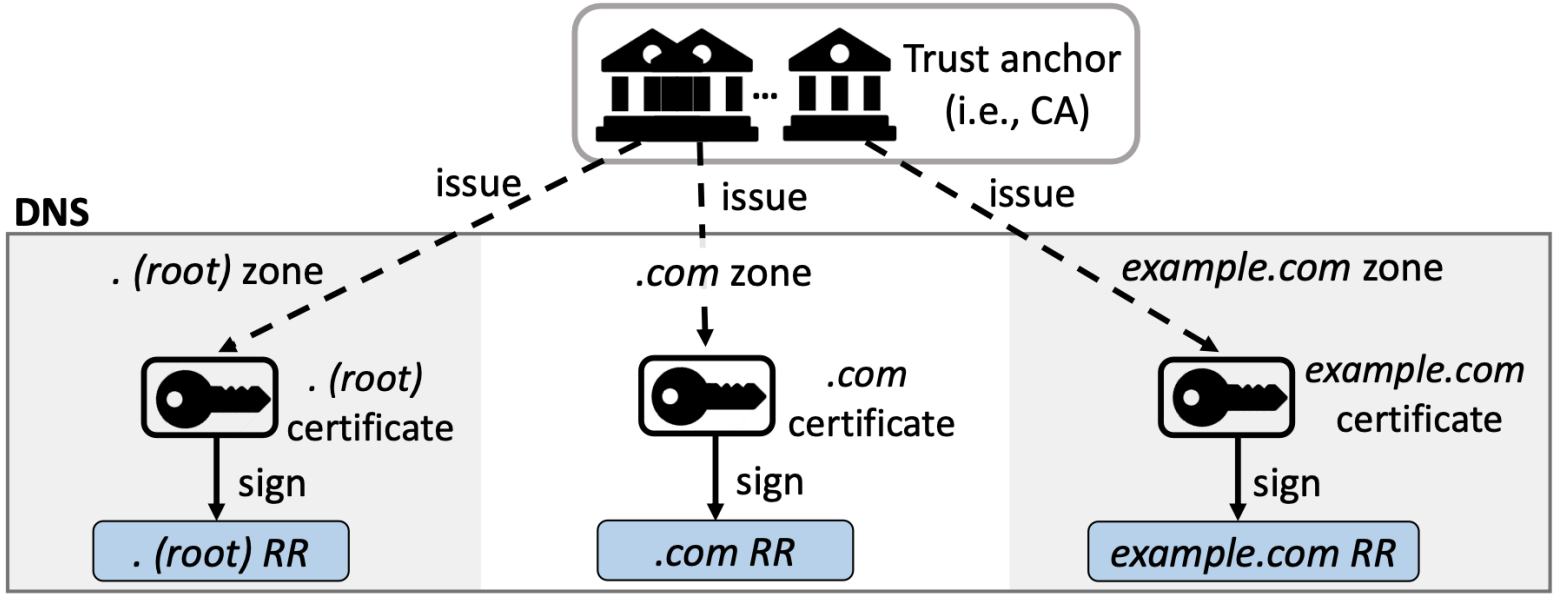
[3] https://transparencyreport.google.com/https/overview

Leveraging PKIX Certificates issued by CAs

DNSSEC



Proposal

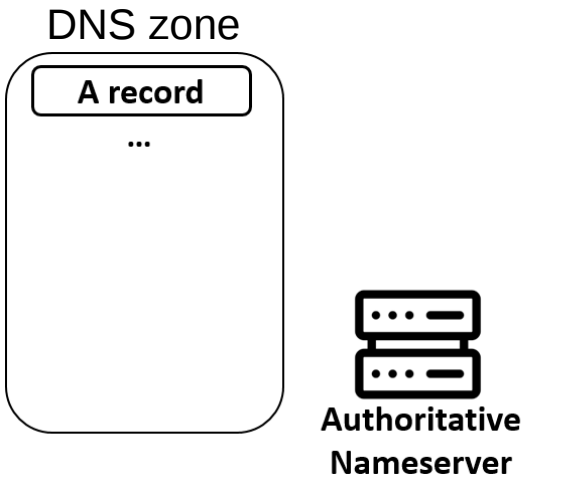


DNSSEC extension for PKIX certificates

We propose to reuse the DNSKEY, RRSIG and CERT records

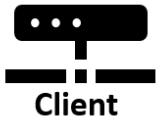
Domain

1. A domain is issued a PKIX certificate (or its TLS one is reused)
2. The domain generates a signature of an RRset using its private key
3. The domain uploads the signature as an **RRSIG** record
4. Also, the domain uploads the public key as a **DNSKEY** record and a certificate chain as **CERT** records



Client-side

i) A client fetches a DNS record (e.g., **A** record) and a signature (**RRSIG**)
ii)The client fetches the public key (**DNSKEY**) and the certificate chain (**CERT**), and validates them through the certificate verification process
iii)The client verifies the signature (**RRSIG**) using the public key



Minimize changes of the entities in DNS infra.

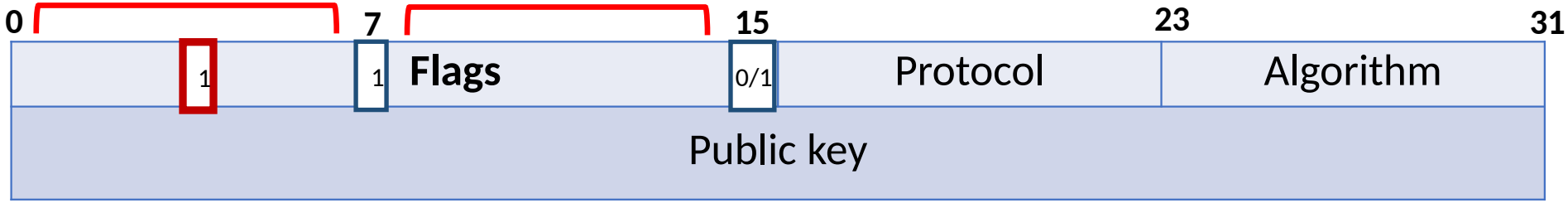
- Our design should **minimally require changes (or cooperations) of other entities in the DNS infrastructure**
  - We leverage CA-issued PKIX certificates (and public/private keys) which are widely used by domains
  - The public key can be verified through the certificate chain verification, which does not require cooperation from other DNS entities
    - cf) DNSSEC requires cooperation from parent zone or registrars to establish a chain of trust due to the DNS hierarchy (e.g., uploading DS records to the parent zone)
  - Only authoritative name servers and local resolvers need to be changed
    - Deploying CERT records (name servers) and verifying a certificate chain (local resolvers)

Reuse DNS record types

- We suggest exploiting existing record types: **DNSKEY, RRSIG,** and **CERT** record
  1. **DNSKEY** stores a public key corresponding to the private key which is used to generate signatures of DNS records

     - **Flags** field [4]
       - Two bits are used in current DNSSEC
         * bit 7 – set to 1? Holds a key for DNS zone
         * bit 15 – set to 1? KSK | set to 0? ZSK
       - Other bits (0-6, 8-14) are **reserved for future use**

     → **We can exploit one of these bits to specify our usage**



  2. **RRSIG** records stores the signatures of RRsets
  3. **CERT** records store a certificate chain

[4] Resource Records for the DNS Security Extensions (RFC 4034)

Conclusion

- We proposed an easier way that guarantees the integrity of DNS messages
  - Most DNS messages in the real-world are not protected
  - Our mechanism minimally requires changes (or cooperations) of other entities in the DNS infrastructure
    - By leveraging PKIX certificates that are already widely used by domains
  - Our mechanism reuses existing DNS record types

Thank you!

Taekyoung (Ted) Kwon
tkkwon@snu.ac.kr, tkkwon98@gmail.com