KISA 한국인터넷진흥원

DNS Tutorial :
DNS 거버넌스, 기술동향

2020. 8. 21.

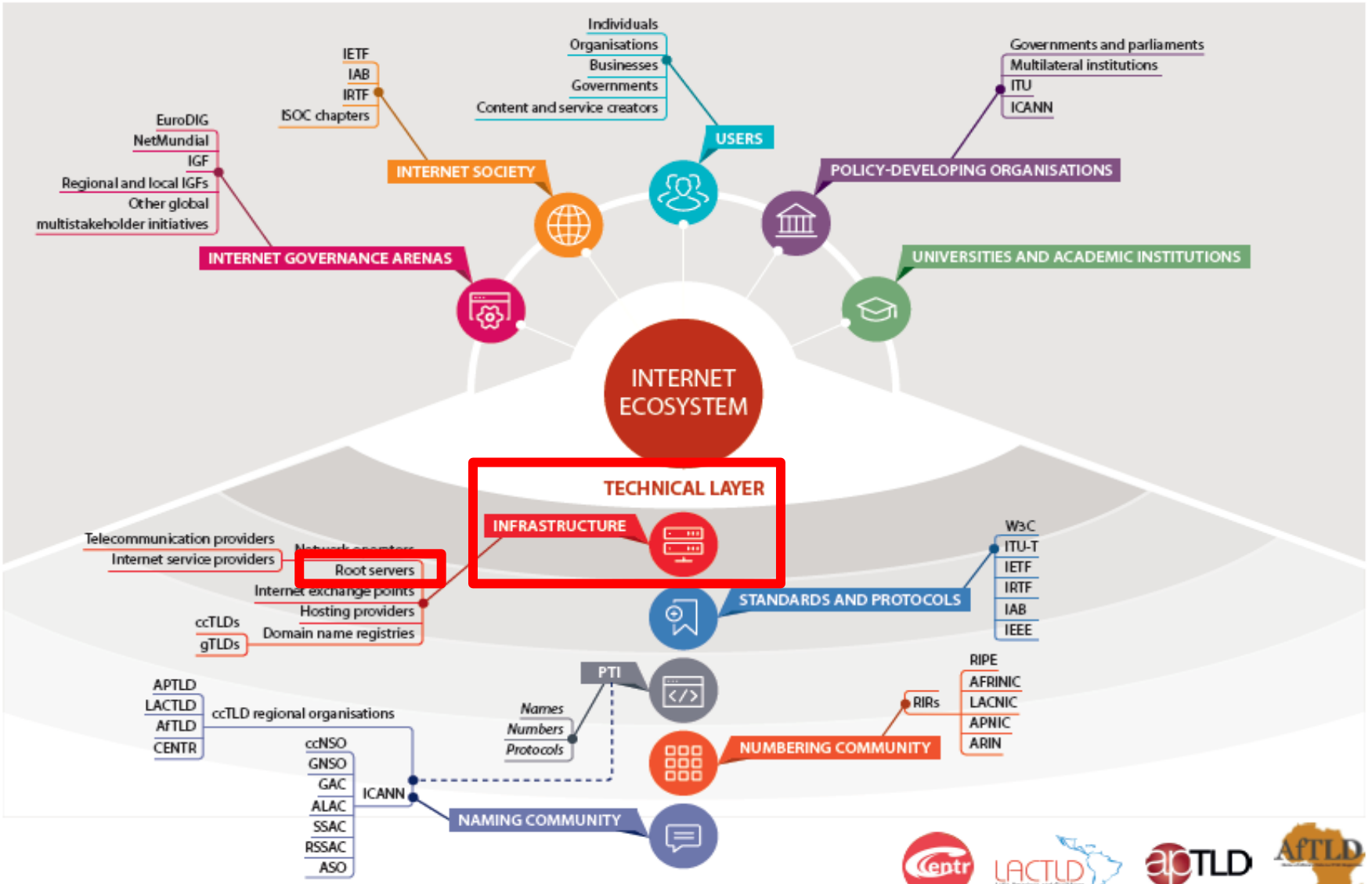
한국인터넷진흥원 인터넷주소기술팀
강상현 선임연구원

Content

KISA 한국인터넷진흥원

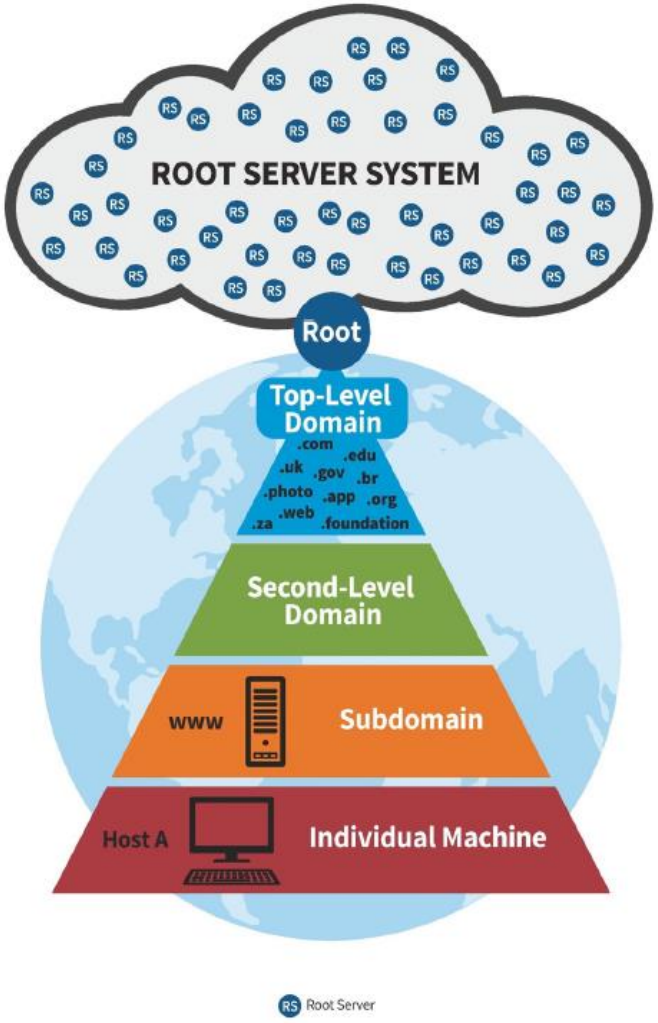
Content

Internet Ecosystem



(Internet Ecosystem, CENTR, 2016)

DNS 생태계



ICANN

iana
Internet Assigned Numbers Authority

RSOs

VERISIGN

USC University of Southern California

cogent

ISC

NASA

...

ccTLD, gTLD

KISA
Korea Internet & Security Agency

denic

CNNIC
中国互联网络信息中心

...

nic.br

.com
powered by VERISIGN

.org

(RSSAC037:A Proposed Governance Model for the DNS Root Server System, ICANN/RSSAC, 2018)

DNS 생태계

- ICANN : 인터넷주소자원에 대한 정책 개발
  - RSSAC(루트 서버 시스템 자문 위원회)

- IANA(Internet Assigned Numbers Authority) 기능
  - Domain Names
    - DNS 루트 존(Root Zone) 관리
    - .int, .arpa 존 관리
    - TLD 데이터베이스 관리 등
  - Number Resources
  - Protocol Assignments

DNS 생태계

- 루트 서버 오퍼레이터(RSOs)
  - Verisign, ICANN, ISC 등 12개 기관
  - 13개 루트 DNS(a~m.root-servers.net) 운영
- ccTLD, gTLD 레지스트리
  - KISA : .kr, .한국 ccTLD DNS 관리·운영
  - Verisign : .com, .net TLD DNS 관리·운영
- 권한 DNS, 캐시 DNS
  - 도메인 등록인, 등록대행자, ISP, 호스팅 사업자, 콘텐츠 프로바이더, …

DNS 생태계

- 누구나 DNS를 운영할 수 있다
  - 루트, TLD는 엄격한 위임 절차에 따라 운영기관이 정해지지만, 그 이하 레벨은 그렇지 않음

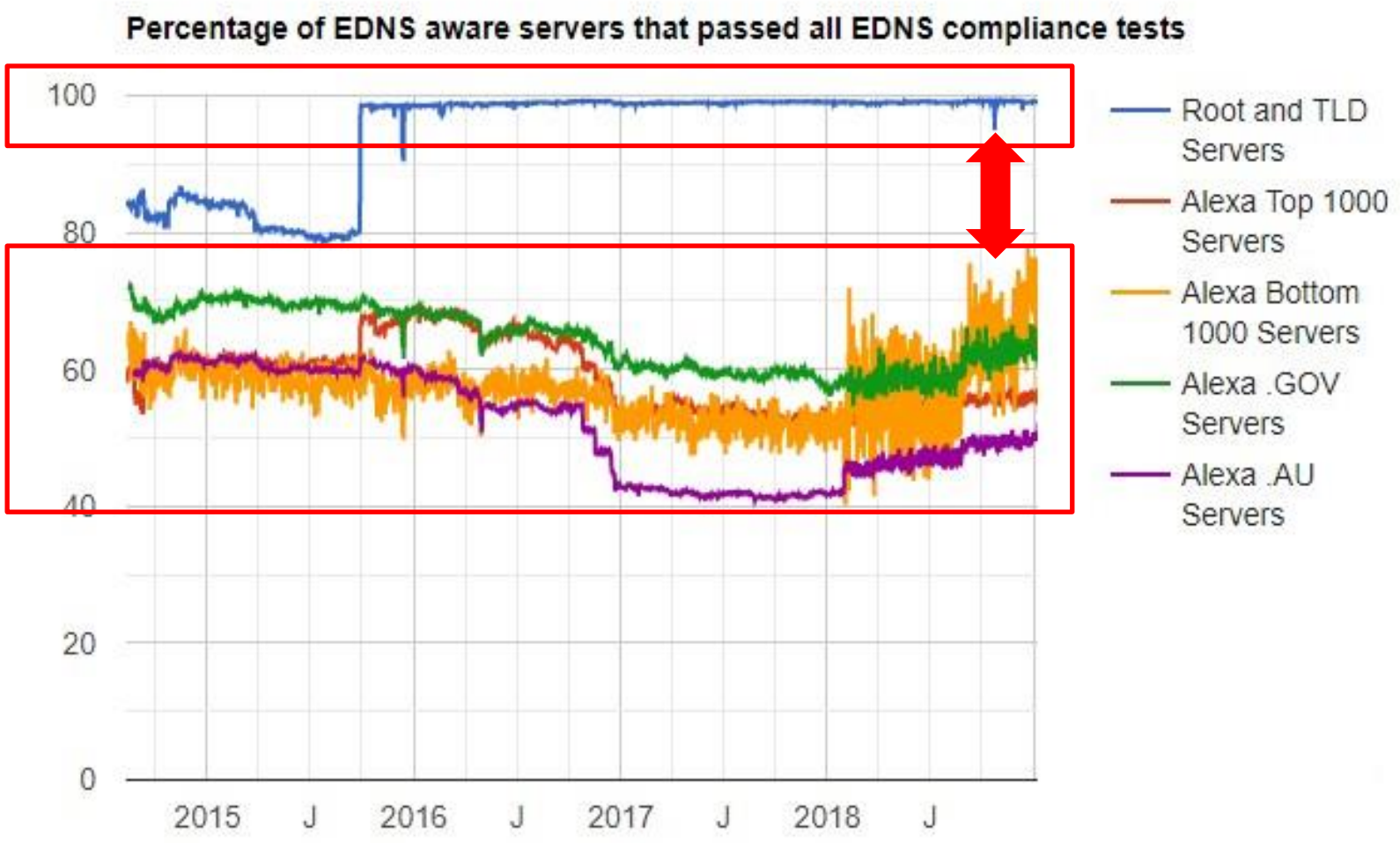
- 관리 체계의 부재
  - 누가 어떤 DNS를 운영하는지 알 수 없으며, 운영에 관여할 방법도 없음
  - DNS 표준은 존재하지만 준수하도록 강제할 방법은 없음

2019 DNS Flag Day

- EDNS (RFC 2671, 6891)는 초기 DNS의 사이즈 제한을 제거하고, 새로운 기능을 추가할 수 있도록 개발된 중요한 DNS 표준으로 1999년 발표됨

- 그러나...

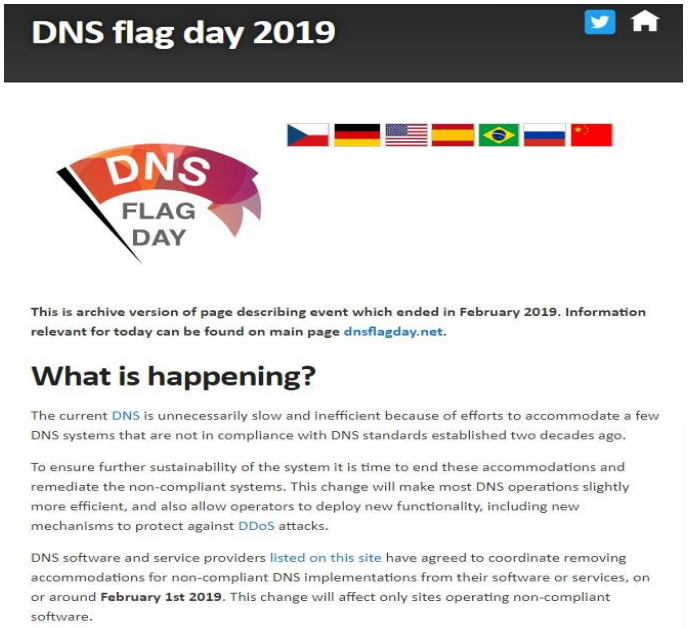
2019 DNS Flag Day

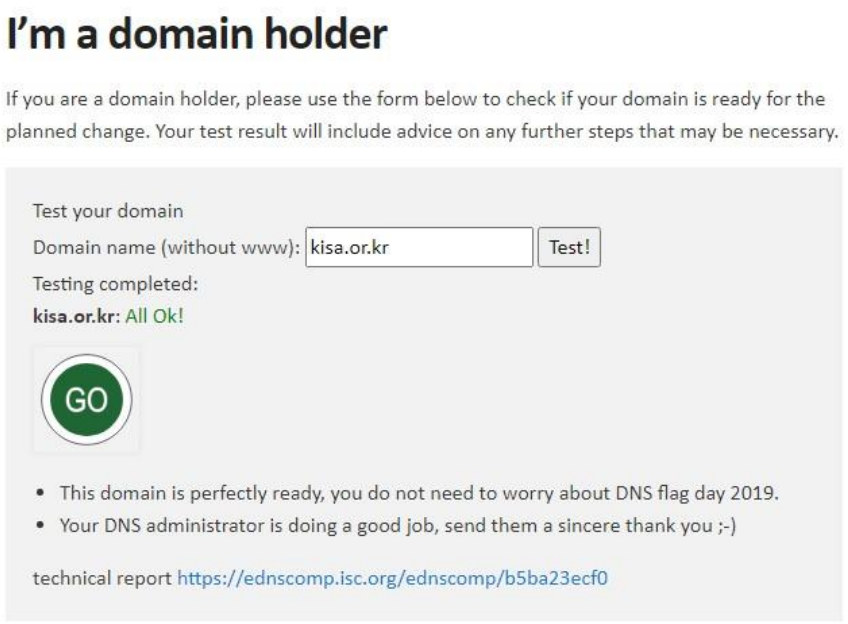


EDNS Compliance Report(https://ednscomp.isc.org/compliance/summary.html), ISC

2019 DNS Flag Day

- DNS S/W 개발사, 글로벌 DNS 운영사, H/W 벤더 등 다양한 이해관계자가 모여 시작된 캠페인
  - 2019. 2. 1. DNS S/W, H/W, 서비스 등 각 영역에서 EDNS 표준을 준수하는 패치와 업그레이드 배포 및 적용

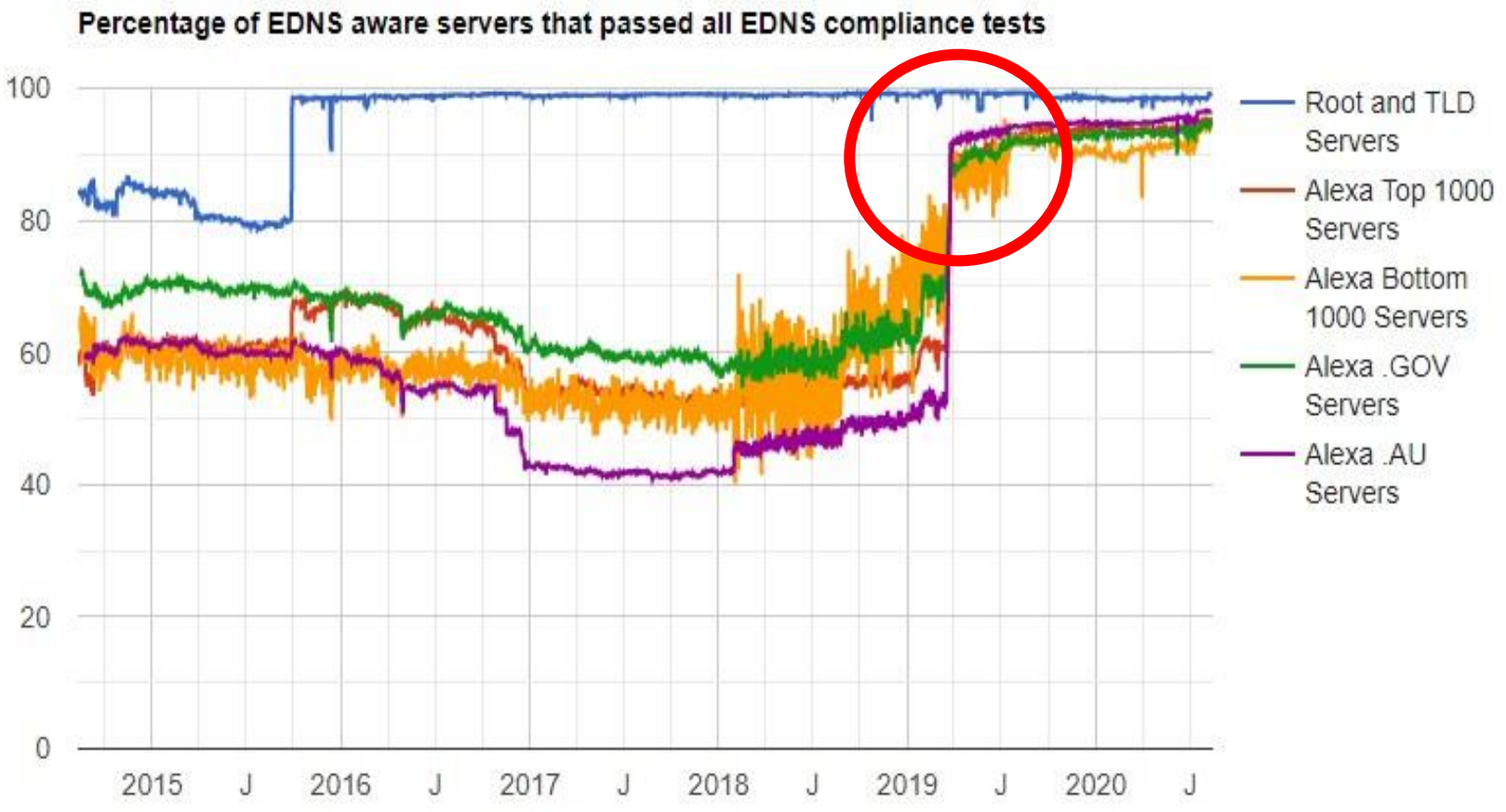




DNS flag day 2019(https://dnsflagday.net)

2019 DNS Flag Day

- 효과는?



EDNS Compliance Report(https://ednscomp.isc.org/compliance/summary.html), ISC

2019 DNS Flag Day

- 다양한 이해관계자가 만들어낸 자발적인 DNS 생태계의 개선 성공 사례

- 메이저 업체를 제외한 소규모 업체나 개인들의 참여를 끌어내지는 못함
  - 주로 DNS-OARC 회원기관 사이에서 논의가 이루어졌으며, 그 외 DNS 운영자나 개인들은 정보를 얻기 어려웠음

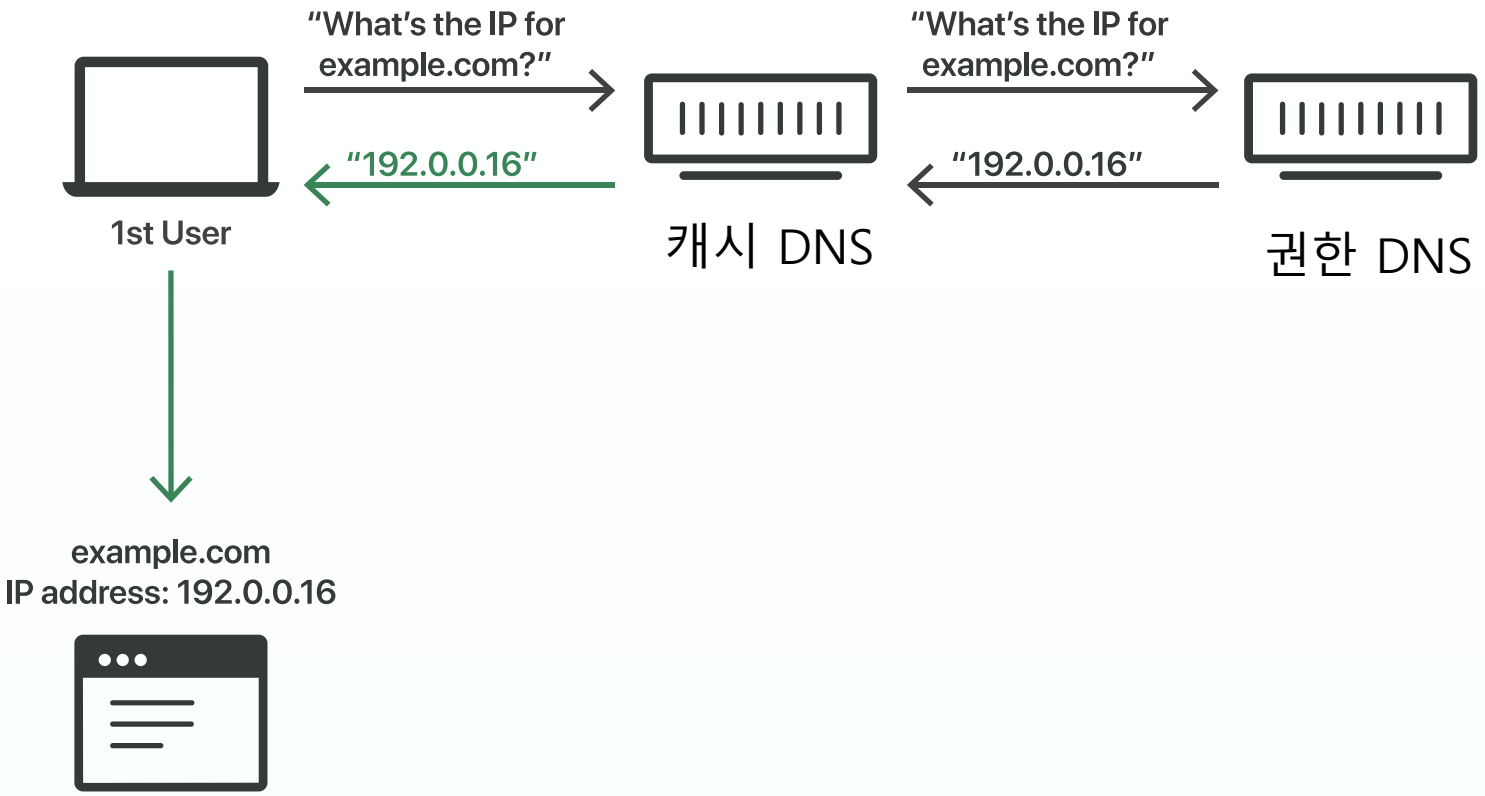
Content

DNS의 근본적 문제점

- DNS는 보안을 고려하지 않고 설계된 프로토콜
- 특히, 주고 받는 DNS 데이터의 진위 여부를 검증할 수 없음
- 만약, 내가 질의한 도메인에 대한 “위조된” DNS 응답을 받았다면…?

DNS 캐시 포이즈닝(Cache Poisoning) 공격

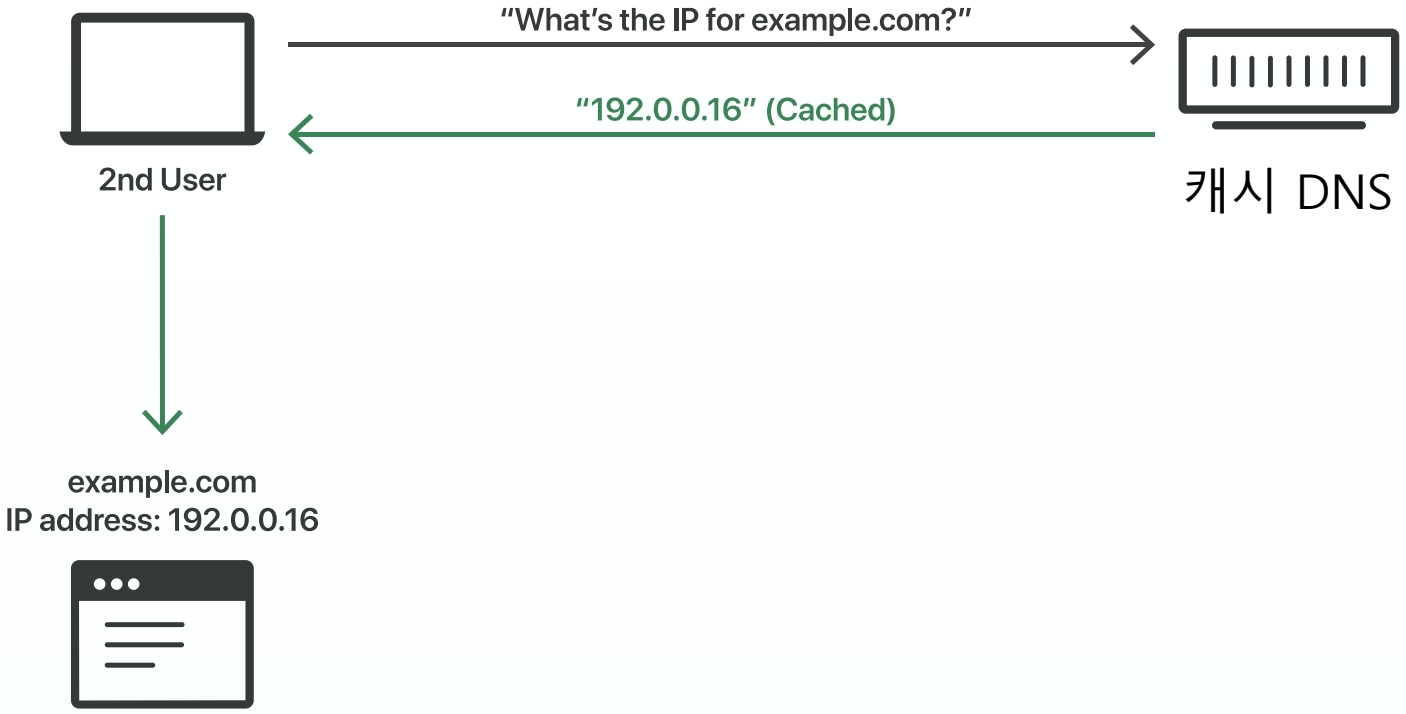
- 정상적인 DNS 질의/응답



What is DNS cache poisoning? (https://www.cloudflare.com/ko-kr/learning/dns/dns-cache-poisoning/), Cloudflare

DNS 캐시 포이즈닝(Cache Poisoning) 공격

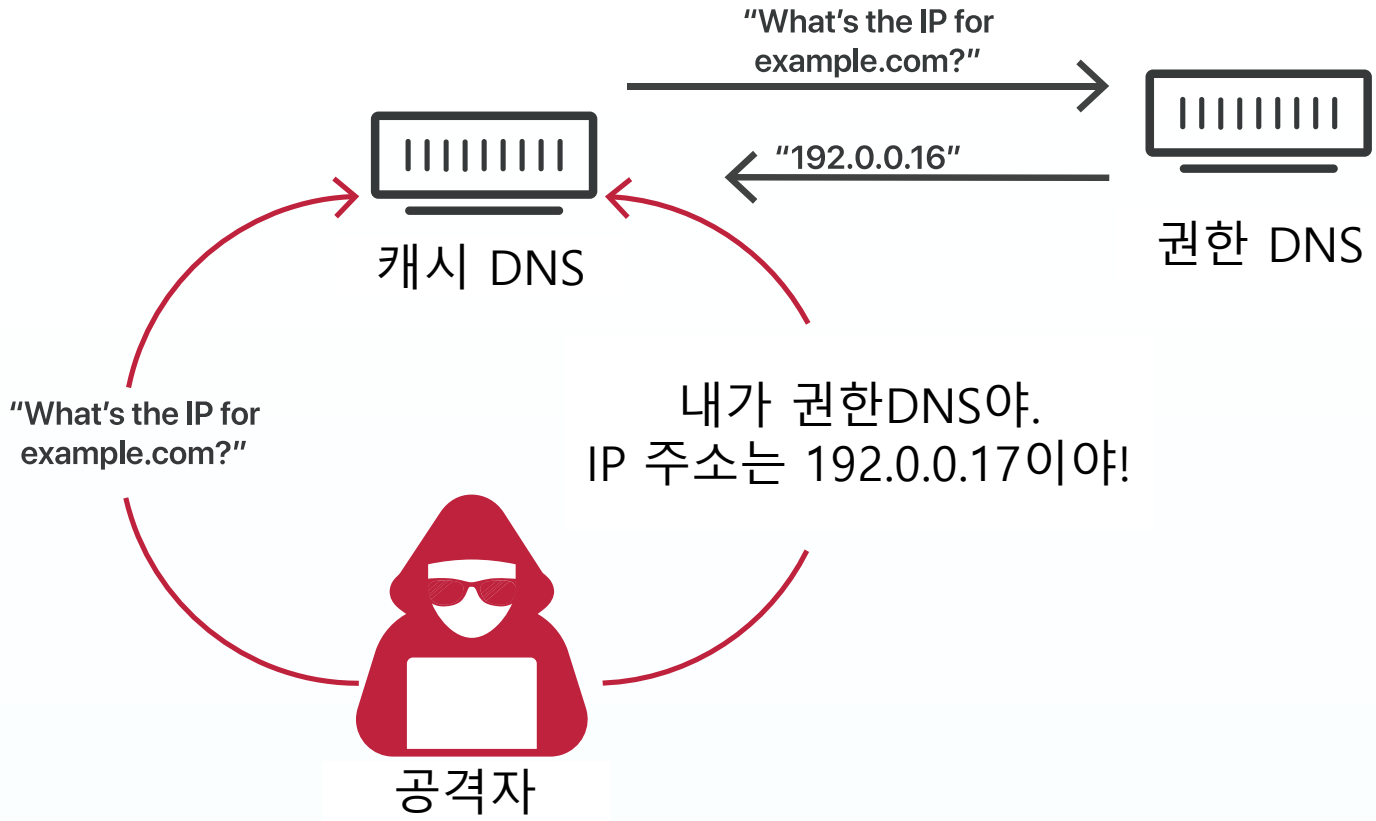
- 정상적인 DNS 질의/응답



What is DNS cache poisoning? (https://www.cloudflare.com/ko-kr/learning/dns/dns-cache-poisoning/), Cloudflare

DNS 캐시 포이즈닝(Cache Poisoning) 공격

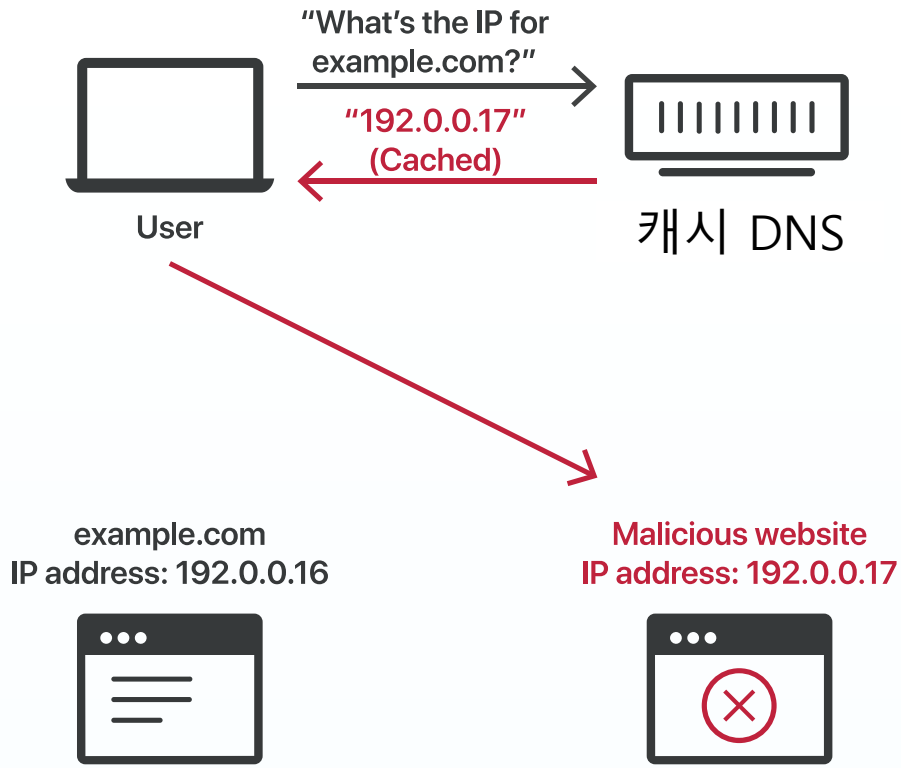
- 위조된 DNS 질의/응답



What is DNS cache poisoning? (https://www.cloudflare.com/ko-kr/learning/dns/dns-cache-poisoning/), Cloudflare

DNS 캐시 포이즈닝(Cache Poisoning) 공격

- 위조된 DNS 질의/응답



What is DNS cache poisoning? (https://www.cloudflare.com/ko-kr/learning/dns/dns-cache-poisoning/), Cloudflare

DNSSEC 동작 원리

- DNSSEC (DNS Security Extension)
- DNS 데이터가 무결함을 증명하려면?
- DNSSEC 서명과 검증
  - 개별 DNS마다 자신의 DNS 데이터가 무결함을 증명할 수 있는 전자서명을 추가 (Signing)
  - 어떤 DNS에서 받아온 DNS 데이터는 그 DNS의 공개키를 이용해 전자서명이 올바른지 검증 (Validation)
  - 검증을 위해 가져온 공개키가 위조될 가능성은?

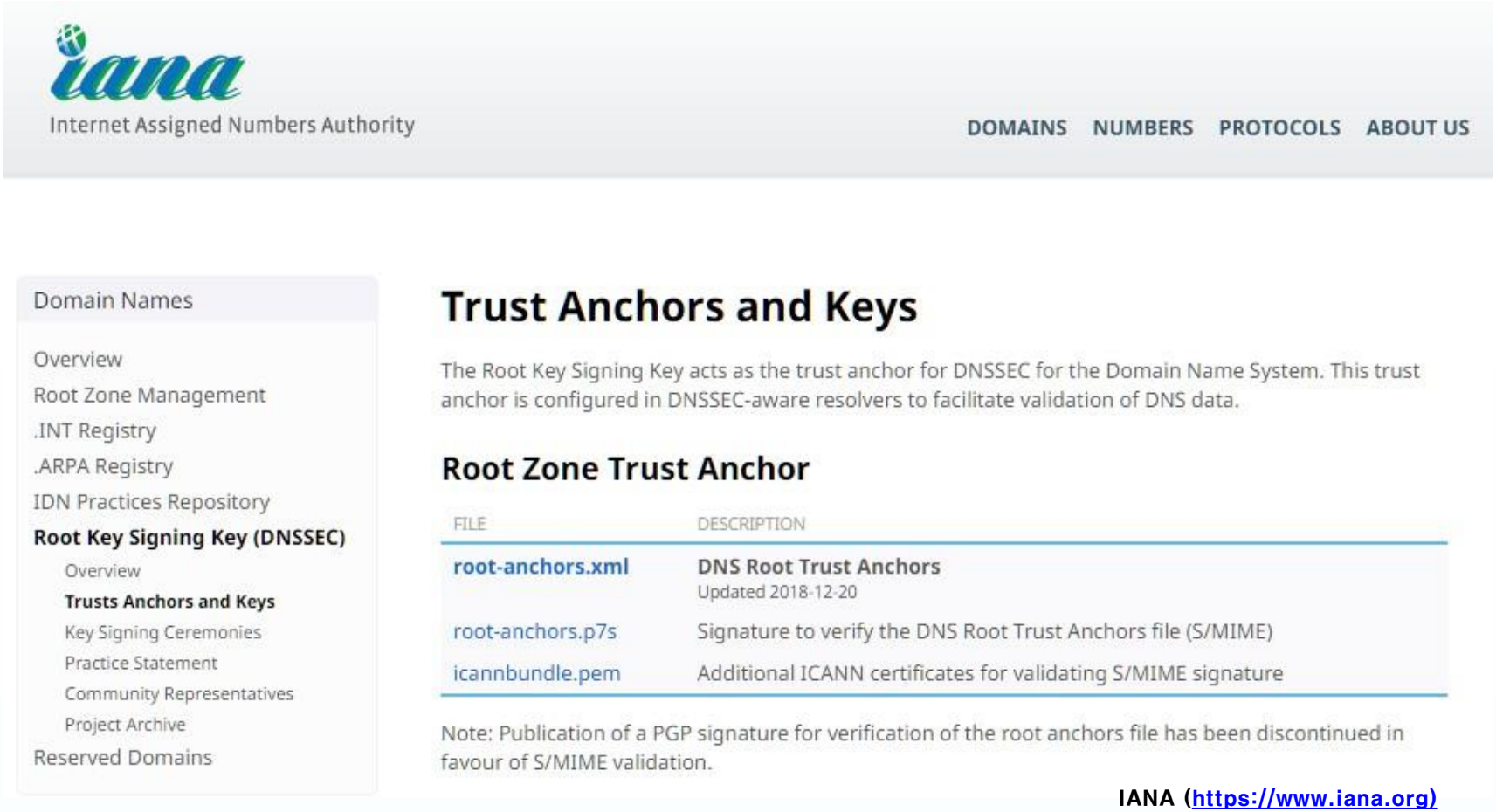
DNSSEC 동작 원리

- 신뢰 체인 (Chain of Trust)
  - 내 DNS의 공개키 정보는, 내 상위 DNS에 등록하여 무결함을 보장받을 수 있음
  - kisa.kr의 공개키 정보는? .kr DNS가 보장
  - .kr의 공개키 정보는? Root(.) DNS가 보장
  - Root(.)의 공개키 정보는??

DNSSEC 동작 원리

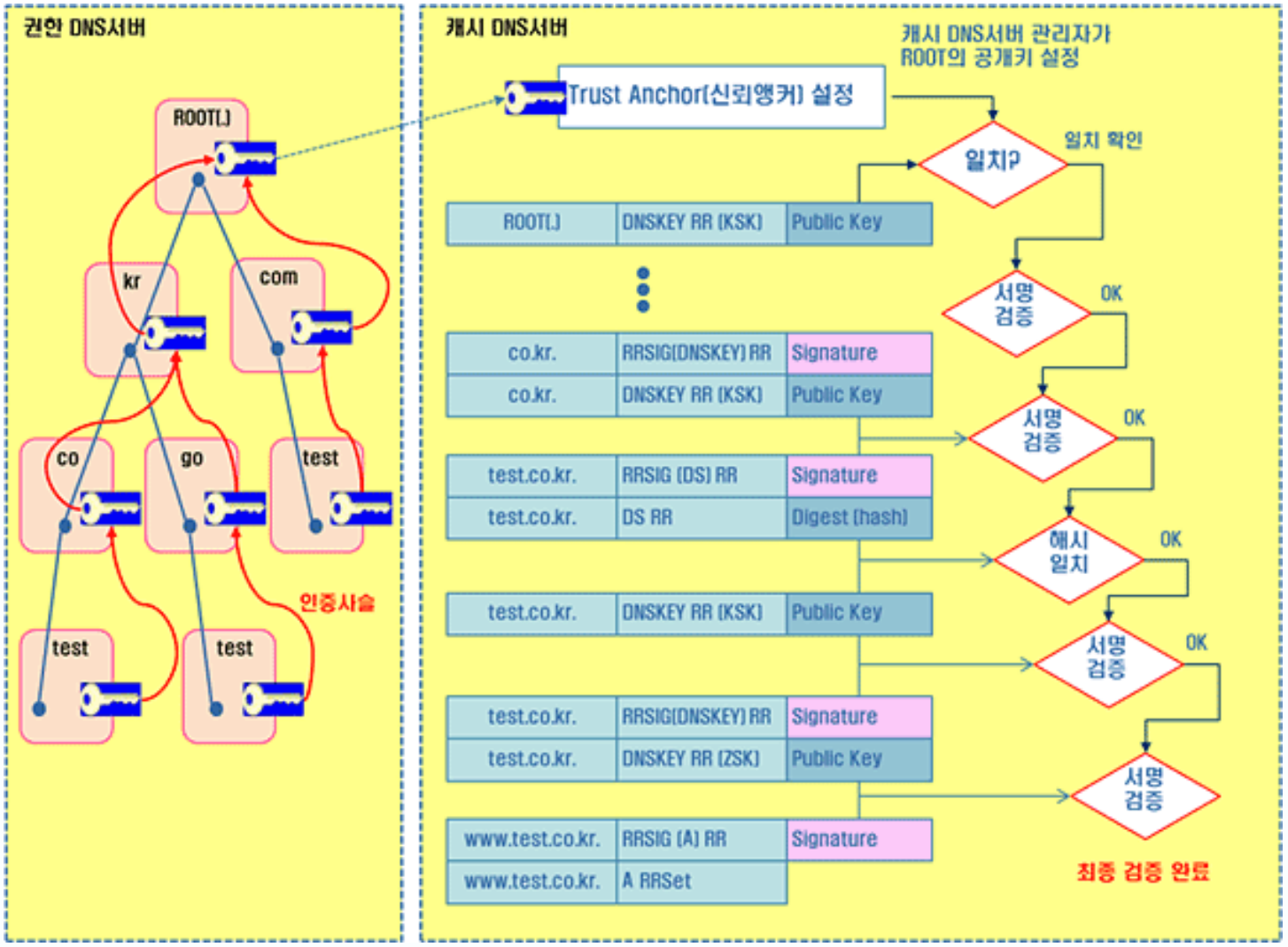
- Trust Anchor (TA)
  - Root(.) DNS는 DNS 체계 최상위에 위치하기 때문에 다른 누군가가 공개키를 보장해줄 수 없음
  - 따라서, DNSSEC 검증이 이루어지려면, Root에 대한 공개키 정보를 별도로 가지고 있어야 함
  - 이 정보를 Trust Anchor 라고 하며, 모든 DNSSEC 검증의 출발점이 됨

DNSSEC 동작 원리



IANA (https://www.iana.org)

DNSSEC 동작 원리


권한 DNS서버
ROOT(.)
kr
com
co
go
test
test
test
인증사슬
캐시 DNS서버
캐시 DNS서버 관리자가
ROOT의 공개키 설정
Trust Anchor(신뢰앵커) 설정
일치?
일치 확인
ROOT(.) DNSKEY RR (KSK) Public Key
서명 검증
OK
co.kr. RRSIG(DNSKEY) RR Signature
co.kr. DNSKEY RR (KSK) Public Key
서명 검증
OK
test.co.kr. RRSIG (DS) RR Signature
test.co.kr. DS RR Digest (hash)
해시 일치
OK
test.co.kr. DNSKEY RR (KSK) Public Key
서명 검증
OK
test.co.kr. RRSIG(DNSKEY) RR Signature
test.co.kr. DNSKEY RR (ZSK) Public Key
서명 검증
www.test.co.kr. RRSIG (A) RR Signature
www.test.co.kr. A RRSet
최종 검증 완료

DNSSEC 도입 경과

- (~2005) DNSSEC 핵심 표준 작업 완료
- (2008 ~ 2010) 루트 존 DNSSEC 초기 도입
  - 2010년 7월, 루트(Root) 존의 DNSSEC 서명
- (2012) .kr, .한국 DNSSEC 서명
- (2015 ~ 2018) 루트 존의 첫번째 서명키 교체

앞으로의 과제

- 여전히 낮은 DNSSEC 도입률
  - TLD 레벨에는 90% 이상 도입 완료
  - 사용자 도메인 레벨은 거의 미도입 상태

    (.com 기준 전체 도메인의 약 1.5% 도입)

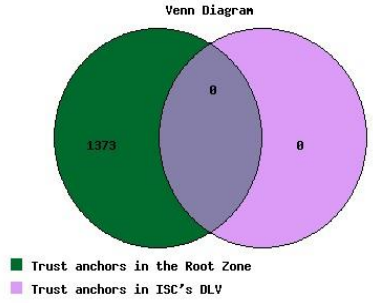
ICANN Research

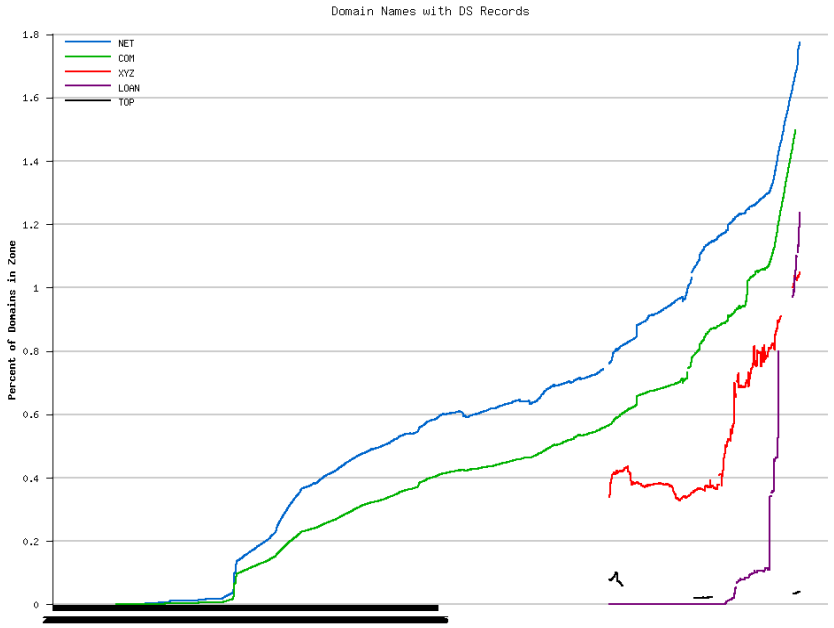
TLD DNSSEC Report (2020-08-16 00:03:05)

[archive] [latest]

Summary

- 1509 TLDs in the root zone in total
- 1383 TLDs are signed;
- 1373 TLDs have trust anchors published as DS records in the root zone;
- 0 TLDs have trust anchors published in the ISC DLV Repository.





Content

DNS와 프라이버시

- DNS는 보안을 고려하지 않고 설계된 프로토콜
- DNS 데이터의 위변조는 DNSSEC으로 검증 가능,
  그러나 누군가 훔쳐보는 것을 막을 수는 없음
  - DNS 통신 구간 암호화의 부재
- 해결방안은? DNS 통신 전체의 암호화

DNS와 프라이버시

- DoT? DoH?
  - DoT (DNS-over-TLS)
  - DoH (DNS-over-HTTPS)

- 목적은 동일, 방법에는 차이

DNS와 프라이버시

- DoT (DNS-over-TLS)
  - 전용포트 TCP 853, TLS 암호화 채널 사용
  - DNS 트래픽을 별도로 분리하여 관리 가능
- DoH (DNS-over-HTTPS)
  - 기존 웹과 동일한 TCP 443, HTTPS 암호화 사용
  - DNS와 웹 트래픽이 구분되지 않음
- DNS 트래픽을 구분할 필요가 있는가?
  - 네트워크 관리자의 보안 모니터링

    vs. 인터넷 검열, 프라이버시 침해

DNS와 프라이버시


Experiments
Chrome | chrome://flags/#dns-over-https
Search flags
Reset all
When enabled, Chrome may query a configured DoH server for HTTPSSVC records. If any HTTPSSVC records are returned, Chrome may upgrade the URL to HTTPS. If the records indicate support for QUIC, Chrome may attempt QUIC on the first connection. – Mac, Windows, Chrome OS, Android
#dns-httpssvc
Default
Secure DNS lookups
Enables DNS over HTTPS. When this feature is enabled, your browser may try to use a secure HTTPS connection to look up the addresses of websites and other web resources. – Mac, Windows, Chrome OS, Android
#dns-over-https
Default
Web Bundles
Enables experimental supports for Web Bundles (Bundled HTTP Exchanges) navigation. – Mac, Windows, Linux, Chrome OS, Android
#web-bundles
Default

DNS와 프라이버시

- DoT/DoH로 DNS는 완전히 보호되는가?
  - 도청으로부터는 안전, DNS 데이터의 무결성을 여전히 DNSSEC 필요
- 어떤 캐시DNS를 사용할 것인가?
  - 캐시DNS는 암호화된 DNS 질의 내용을 볼 수 있음
  - 캐시DNS의 신뢰도 문제

DNS 데이터 활용

- DNS는 인터넷 연결의 출발점이며, 모든 도메인 기반 연결 시 반드시 거쳐가는 서비스

- 그렇다면, DNS 데이터를 분석하면 뭔가 새로운 것을 찾을 수 있지 않을까?

DNS 데이터 활용

- Passive DNS
  - DNS 질의/응답 히스토리를 기록한 데이터베이스
  - 언제, 어떤 도메인이, 어떤 타입에, 어떤 응답을 했는지
  - 일종의 DNS 아카이브

  - (예) www.kisa.or.kr 의 IP 주소가 10.10.10.10 이었는데, 특정 시기에 20.20.20.20 으로 바뀌었다가, 다시 며칠 뒤 10.10.10.10이 되었다면?

DNS 데이터 활용

Successful Query for: pom-pharmacy.com A (Limit 50000)

EXPORT AS CSV | EXPORT AS JSON | API DOCS

Show 25 entries

Time Last Seen	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2019-05-06 14:14:04	2017-10-06 17:20:44	1377	pom-pharmacy.com.	pom-pharmacy.com.	A	66.212.148.115
2017-09-26 12:28:46	2017-03-17 12:51:24	390	pom-pharmacy.com.	pom-pharmacy.com.	A	74.81.170.110
2017-03-14 22:42:18	2016-08-18 17:33:38	1414	pom-pharmacy.com.	pom-pharmacy.com.	A	104.28.22.110 104.28.23.110
2016-08-17 22:23:15	2016-02-15 00:10:04	1921	pom-pharmacy.com.	pom-pharmacy.com.	A	185.92.221.211
2016-02-14 21:56:42	2013-07-19 01:33:42	12025	pom-pharmacy.com.	pom-pharmacy.com.	A	50.7.195.186

Showing 1 to 5 of 5 entries

First | Previous | 1 | Next | Last

Hunting with Passive DNS, Ben April, Farsight Security, 2019

DNS 데이터 활용

- DGA 도메인 탐지
  - DGA(Domain Generation Algorithm) 도메인 : 일부 악성코드가 명령 서버에 접속하기 위해 사용되는 무작위 생성 도메인

V6PNSC80LL.COM
B9U5R3RJMPP.COM
YM5R99EX5Q8.COM
MBSIGLGFQIH2.COM
GSJZNQCOHIKO.COM
VEG2671WMX88.COM
DLNOYYVQSOZHH.COM
BFZFLQEJOHXMQ.COM
AJFSZWOMNHDFCYY.COM
EXAGQLXTMOPSFT8.COM
FWOGZPAGLGOVLIMY.COM

JVRRMMKYEJDEYLCQ.COM
LKLHJONIUDKKHCWO.COM
CADDBSGSCNYDZOH5F.COM
CEUNNFOHGWJYAUA9H.COM
NQZHTFHRMYMTVBQJE.COM
OVLREWGRHHVAJBOTX.COM
OTPWFJOKPOZOOMNK2O.COM
CNEISZDKHZEKQEUBUT.COM
EMUXMJDBTNWCQRFN0G.COM
OWASALWIGURWYVNNPV.COM
PMNYPARTDBVYHCZDJS.COM

  - DNS 질의 내역에서 사람이 사용하지 않을 법한 도메인을 뽑아보면 어떨까?

좀 더 범용적인 DNS

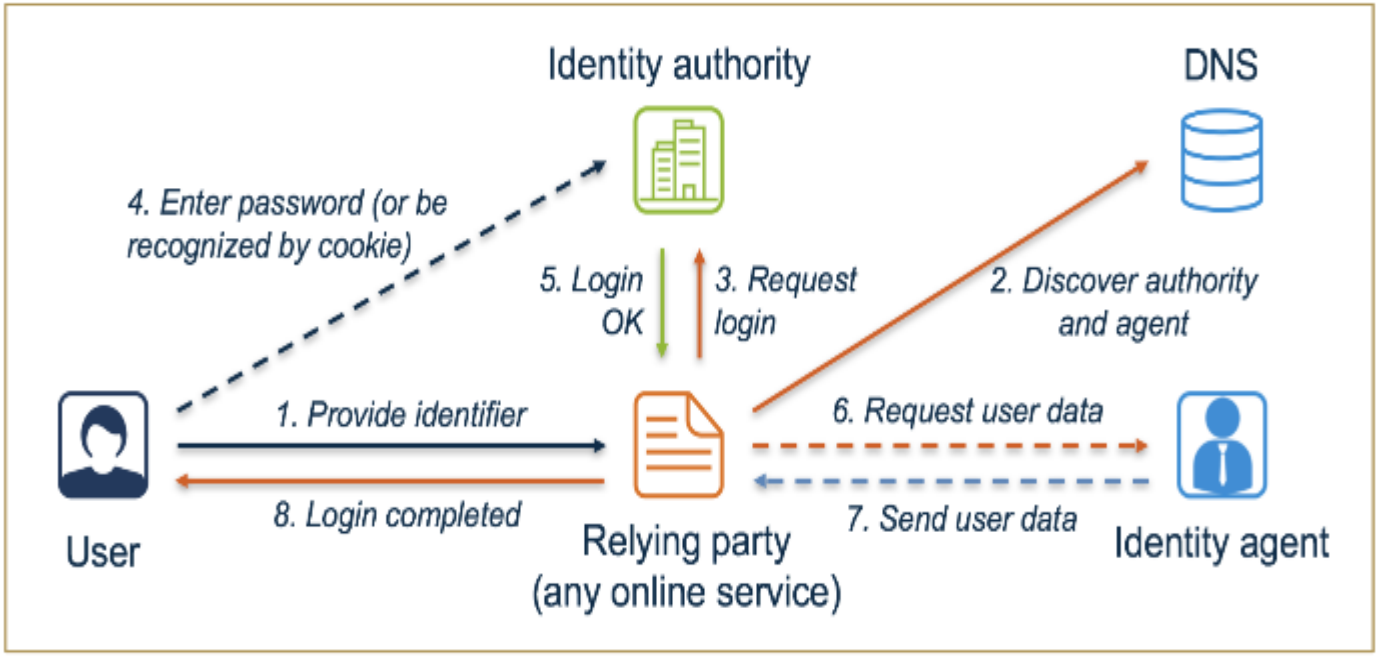
- DNS의 기본 동작은 도메인 – IP주소 간 매핑과 변환
  - 도메인은 Key이며, IP주소는 Value로 볼 수 있음
- 그렇다면, IP 주소가 아닌 다른 것을 넣어주면?
  - 거대한 분산 DB로서 DNS 활용 가능성

좀 더 범용적인 DNS

- DANE (DNS-based Authentication of Named Entities)
  - DNS를 서버 인증 정보를 교환하는 수단으로 활용
  - 인스턴트 메시징, 메일, VoIP 등 “안전한” 연결이 필요한 다양한 분야에서 활용 가능

좀 더 범용적인 DNS

- ID4me (독일)
  - DNS를 기반으로 구현한 디지털 신원 인증 서비스



ID4me Technical Overview v1.4 (https://gitlab.com/ID4me/documentation/blob/master/id4me%20Technical%20Overview%20v1.4.pdf), ID4me.org

좀 더 범용적인 DNS

- 새로운 서비스를 위해 특정한 타입을 새로 할당하거나, 사전에 약속된 서브도메인을 만드는 형태가 많음
  - DANE – TLSA 레코드
  - _service.example.com
- 다만, 아직 대중적으로 널리 사용되는 서비스는 없음
  - 특히, 데이터 무결성을 위해서는 DNSSEC이 선결 조건

KISA 한국인터넷진흥원

Internet On, Security In!

shkang@kisa.or.kr

감사합니다