Measuring DANE TLSA Deployment

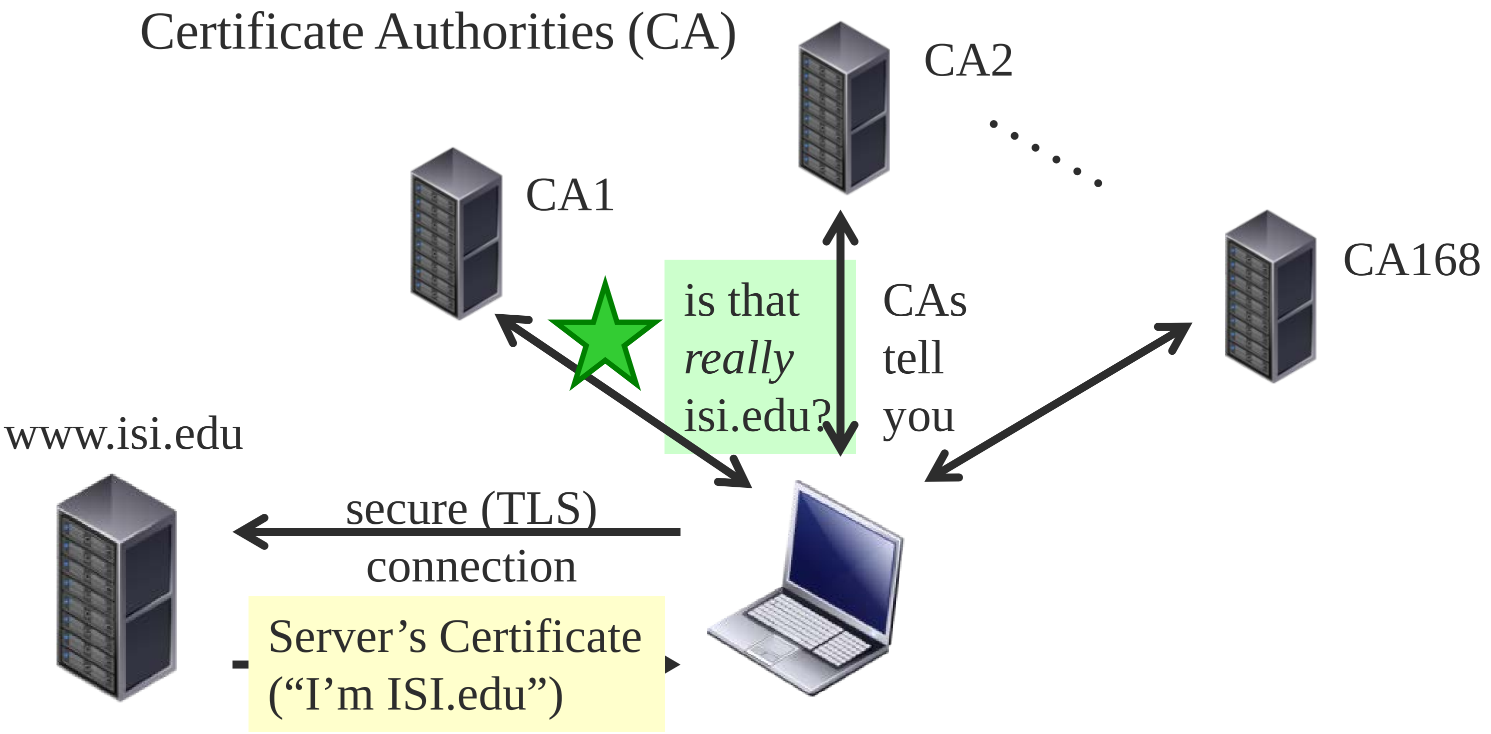
Liang Zhu[1], Duane Wessels[2], Allison Mankin[2], **John Heidemann[1]**

1: USC/Information Sciences Institute; 2: Verisign Labs

2015-04-24

This research is sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, HSARPA, Cyber Security Division, BAA 11-01-RIKA and Air Force Research Laboratory, Information Directorate under agreement number FA8750-12-2-0344, and contract number D08PC75599. The U.S. Gov't is authorized to reproduce and distribute reprints for Gov't purposes notwithstanding any copyright notation thereon. The views herein are those of the authors and do not necessarily represent those of DHS or the U.S. Gov't.

The Challenge of Trust in Certificate Authorities



Certificate Authorities (CA)

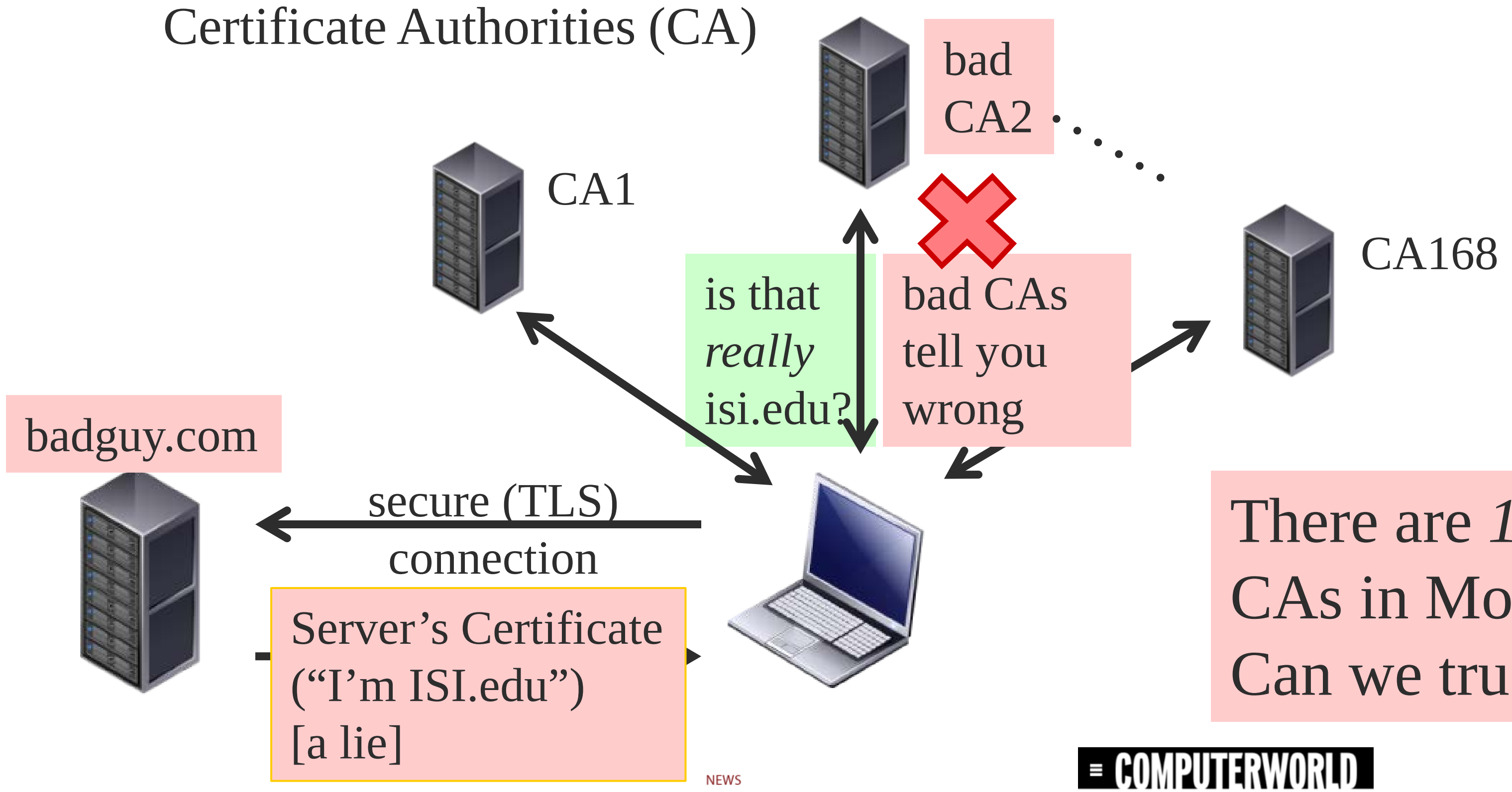
is that *really* isi.edu?

CAs tell you

secure (TLS) connection

Server’s Certificate (“I’m ISI.edu”)

The Challenge of Trust in Certificate Authorities



is that *really* isi.edu?

bad CAs tell you wrong

secure (TLS) connection

Server’s Certificate (“I’m ISI.edu”) [a lie]

There are *168* CAs in Mozilla. Can we trust *all?*

COMPUTERWORLD

NEWS

DiigiNotar dies from certificate hack caper

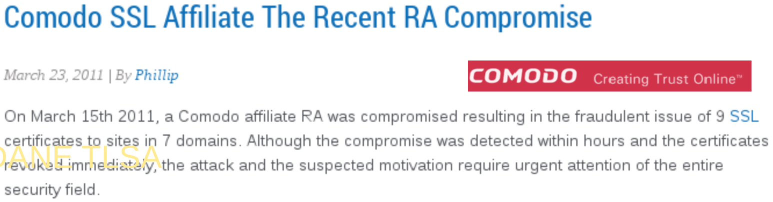
By Gregg Keizer FOLLOW

Computerworld | Sep 21, 2011 5:09 PM PT

techie buzz
know your technology head on.

Gmail Users in Iran Hit by MITM Attacks

By Sathya Bhat on August 30th, 2011

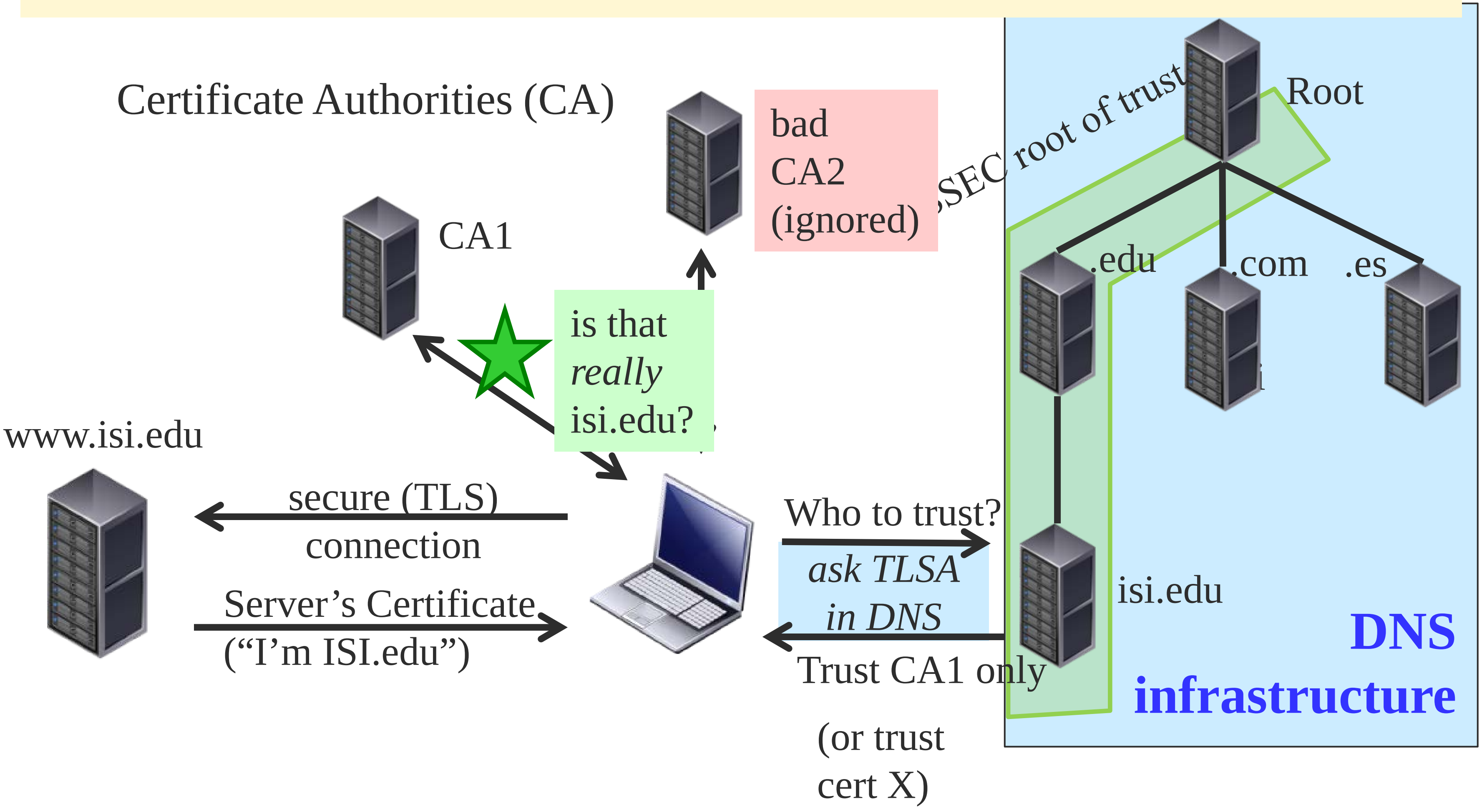

Comodo SSL Affiliate The Recent RA Compromise

March 23, 2011 | By Phillip

COMODO Creating Trust Online™

On March 15th 2011, a Comodo affiliate RA was compromised resulting in the fraudulent issue of 9 SSL certificates to sites in 7 domains. Although the compromise was detected within hours and the certificates revoked immediately, the attack and the suspected motivation require urgent attention of the entire security field.

DANE TLSA **Complements** CAs



But… is DANE TLA *in Use*?

- no systematic study of DANE TLSA use
  - (an informal survey: https://www.tlsa.info/statistics/best_results)

- **our Q: how is DANE TLS *really* used?**
  - how much? correctly? what options?
- can we see DANE take off?

Contribution: First Systematic Measurement of DANE TLSA

- observing TLSA in .com and .net
  - – efficient survey method
  - – shows TLSA use is early but growing
- data on use *correctness*
  - – 7-13% of records seem wrong
- data on response sizes (with DNSSEC)
  - – 33% of require IP fragmentation with UDP

Goals for Measuring TLSA Use

- **complete** (as much as possible)
- **longitudinal** (many measurements)
  - not just one shot
- **efficient**
  - easy to deploy observation system
  - repeatable
  - cheap (can run every day)

Measuring TLSA Use: Passive or Active?

- **passive**: watch resolver traffic (or web crawls)
  - pros: could across the entire DNS namespace
  - cons:
    - missing unused ones => ***incomplete***
    - many vantage points, complex and unreliable => ***inefficient***
- **active**: probe all names in some zone
  - pros:
    - **all** possible names in zone => ***more complete***
    - one probe point, controllable probing cycle => ***efficient***
  - cons: gets only zones under study (not all)
    - most of ccTLD zone files are not available

Our Approach: Actively Scan Zones

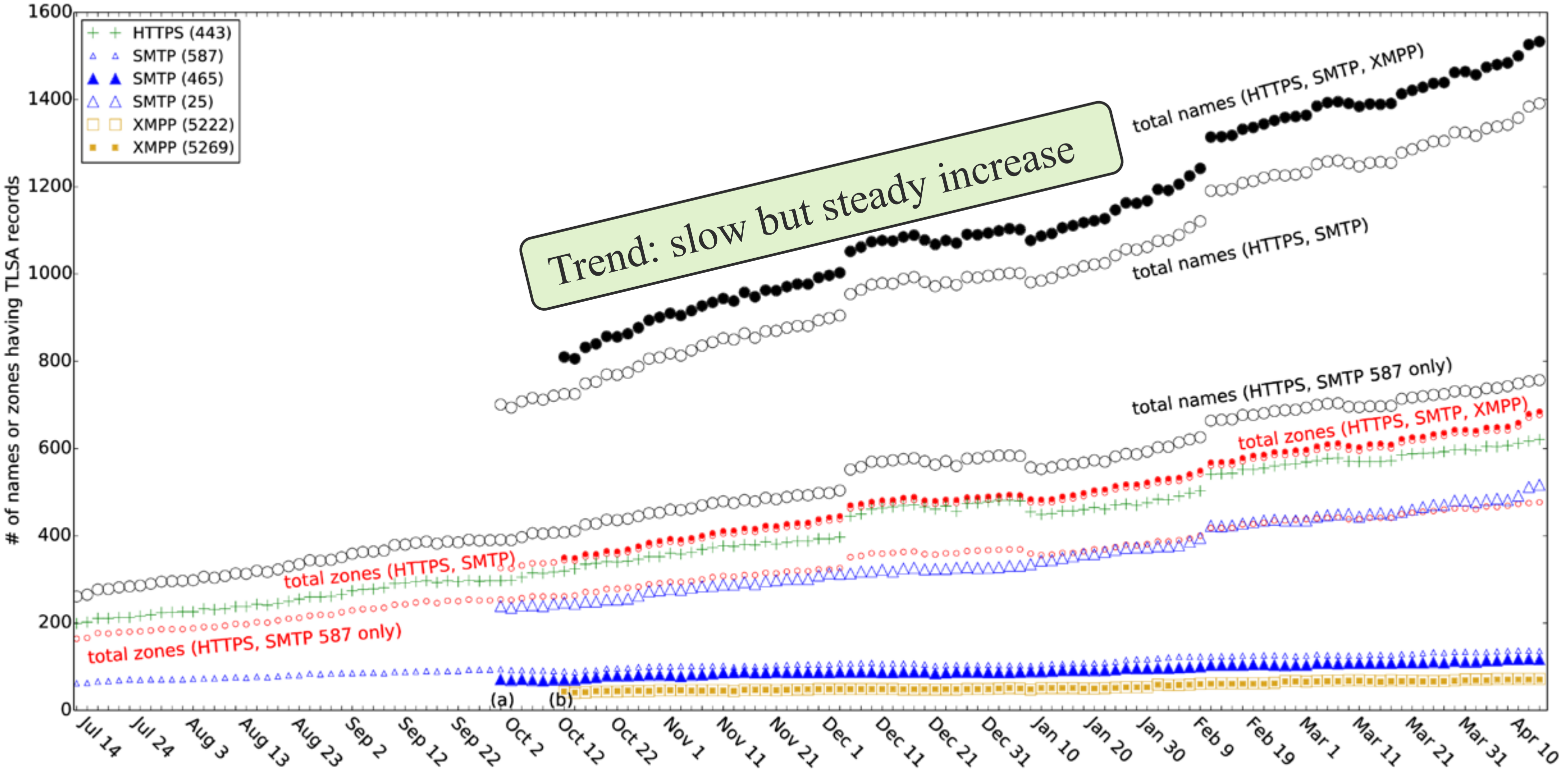
- targets: .com and .net
  - easy to get bulk access
  - complete coverage of these zones
- subset: DNSSEC only
- subset: certain ports
  - https (443)
  - smtp (25, 465, 587)
  - xmpp (5222 , 5269)

```
for ALL DS records in com&net zones
    extract  $DOMAIN     //DNSSEC signed
    check _443._tcp.$DOMAIN
    check _443._tcp.www.$DOMAIN
    for SMTP port 25, 465, 587
        if MX record
            check _$PORT._tcp.$MX
        if no MX record
            check _$PORT._tcp.$DOMAIN
    for $NAME in _xmpp-{client, server}._tcp.$DOMAIN,
            if $NAME SRV record has ($PORT, $TARGET)
                check _$PORT._tcp.jabber.$DOMAIN
            if no $NAME SRV
                for $PORT 5222, 5269
                    check _$PORT._tcp.jabber.$DOMAIN
                    check _$PORT._tcp.xmpp.$DOMAIN
```

Findings and Observations

- how many TLSA names?
- growth in TLSA use ?
- TLSA correctness?
- TLSA parameters and modes?
- TLSA reply size (fragmentation)?

How Many TLSA Names?



Trend: slow but steady increase

Figure only shows data every other day

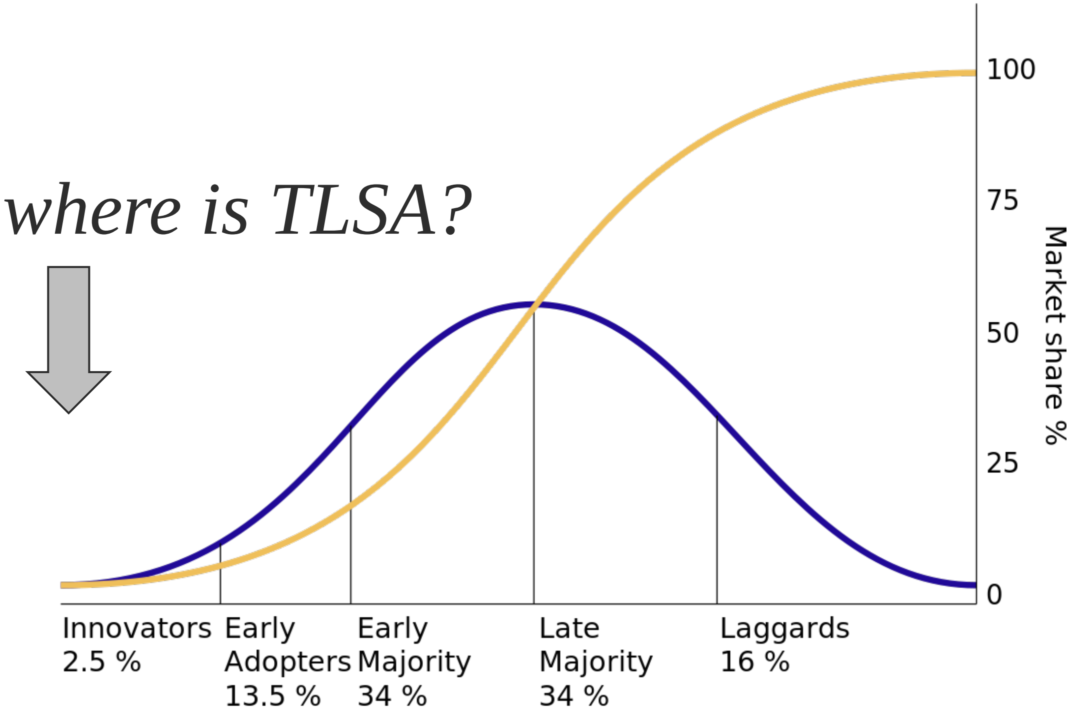
DANE TLSA use is early

- as of 2015-04-17: only 1533 TLSA names in 541k signed zones

Measuring Adoption

penetration := fraction of possible users that use it

where is TLSA?



method:
compare DANE TLSA
(2 years after standardization; population: all DNSSEC)

to DNSSEC
(9 years after standardization; population: all DNS)

TLSA Penetration

zone	N_{all}	N_{dnssec}	N_{tlsa}	P_{dnssec} $(\frac{N_{dnssec}}{N_{all}})$	P_{tlsa} $(\frac{N_{tlsa}}{N_{dnssec}})$
com	117.9M	456k	312	.00387	.00068
net	15.1M	85k	253	.00562	.00298

data as of 2015-04-17:

DANE TLSA: off to a start (but << up to $^{1}/_{3rd}$% of potential)

but still immature (2 years after standardization)

DNSSEC: deployment is still modest (up to ½ % of potential),

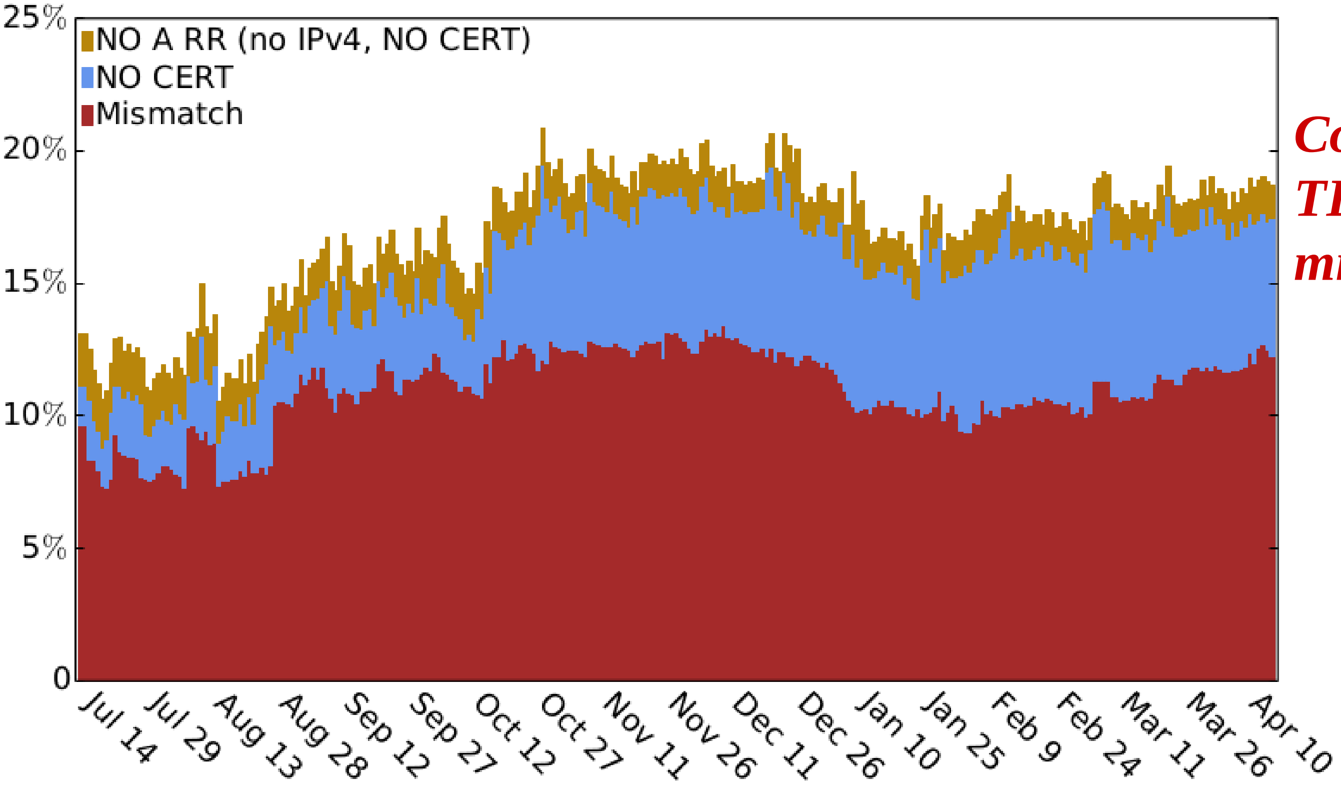
9 years after standardization (~3.5 years after .com and .net signed)

(the DNS community seems slow to change)

Is DANE TLSA Used Correctly?

Validate TLSA records assuming DNSSEC integrity for simplicity

- No cert/No A record: DANE TLSA does not work even deployed
- Mismatch: cert in DANE vs. at server => the use of DANE TLSA will ***fail***



Consistently, 7%-13% TLSA records are mismatched

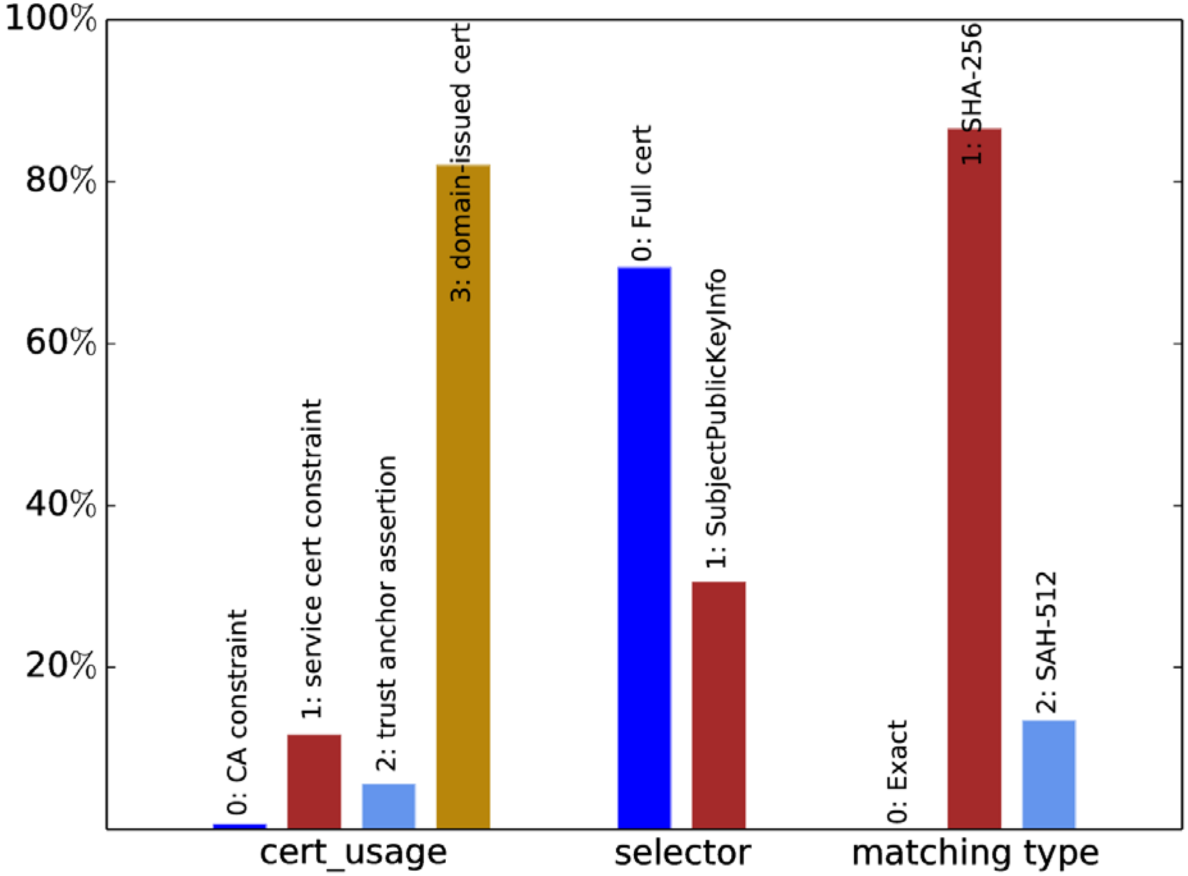
(ports 443 and 587 only)

IPv4 and IPv6: do they match?

- problem: one TLSA record, but two different certificates
  - with usage “domain-issued certificate”
  - TLSA validation must ***fail*** for one cert
  - (possible cause: operators rolled certs and forgot one)
- rare (15 out of 390), but not zero
  - ***need to pay attention***
  - suggests either TLSA or IPv6 is not much used

Data: separate measurement (2014-10-01)

Observed TLSA Parameters



Domain-issued cert: ***most DANE TLSA cases are independent of CA*** without serving its trust source

SHA-256: ***currently strong enough;*** use of SHA-512 not currently necessary

total 1727 TLSA records in 1533 TLSA responses captured on 2015-04-17

Problematically Large Responses

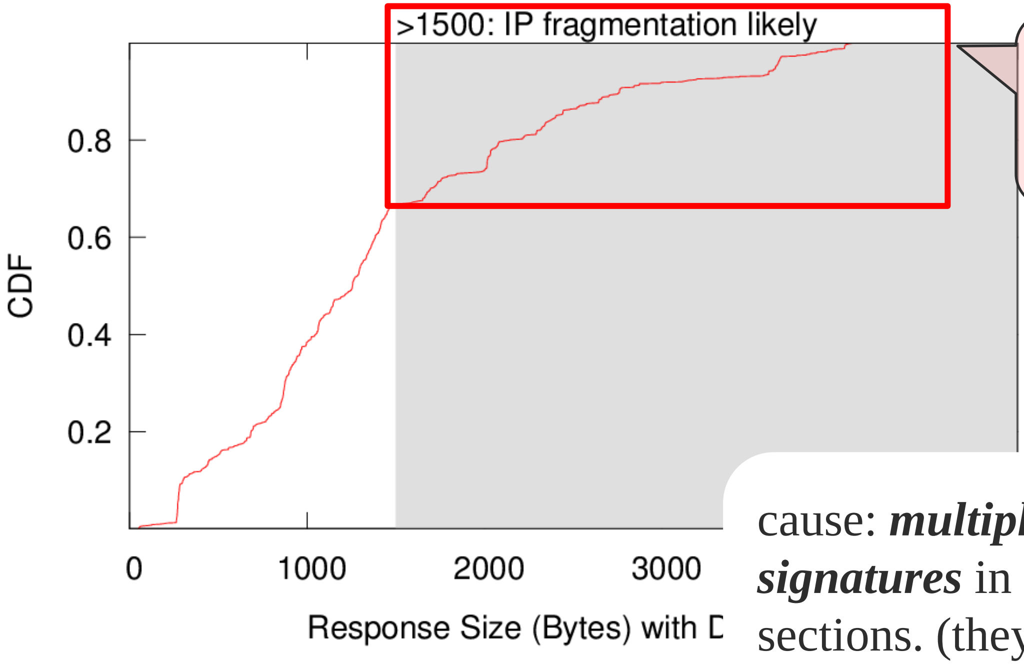
Large DNS packets with UDP: more than 1500 Bytes => IP fragmentation

Problems:

- Risk of fragmentation attack [2]
- Add extra latency of resending due to lost fragments

[2] A. Herzberg and H. Shulmanz. Fragmentation considered poisonous. IEEE Conference on Communications and Network Security, Oct. 2013.

Query TLSA record with DNSSEC to authoritative servers of the 997 TLSA names on Dec. 3, 2014



33% TLSA responses >1500 bytes => fragementation

cause: ***multiple RRs and DNSSEC signatures*** in authority and additional sections. (they give options, but may cause fragementaiton)

Conclusions

- regular tracking of DANE TLSA use
  - DANE TLSA use is early, but growing
  - 7-13% of TLSA records are invalid
  - 33% replies force fragments
- potential TLSA auditing
  - IPv6 certificate validation
  - could check other RR types: OPENPGPKEY
- plans to open-source software and data
- feedback or interest?