Measuring DANE TLSA Deployment

Liang Zhu[1], Duane Wessels[2],

Allison Mankin[2], John Heidemann[1]

1. USC ISI 2. Verisign Labs

DANE is Important

- DANE defines trust for “named entities”
  - Use DNSSEC to prove integrity
  - Named Entities: web sites, email addresses
- Concern about CA trust after multiple compromises
- DANE TLSA complements CAs, allowing owner to describe what they trust
  - Built on DNSSEC's root of trust
  - owners control which CAs, certs, or algorithms to reduce vulnerability

DANE Deployment Status is Unknown

- No systematic study of DANE TLSA deployment
  - ***Few*** prior work [1] tracks TLSA records
- Understand how DANE TLSA has been used
  - Are people using it correctly?
  - What is the common usage?
- Can we see DANE take off?

[1] https://www.tlsa.info/statistics/best_results

Contribution: First Systematic Measurements of DANE TLSA

- Observe TLSA deployment in .com and .net
  - Current DANE TLSA use is early but grows
- We look for correctness
  - 7-12% of records seem wrong
- We look at response sizes (with DNSSEC)
  - 31% of require IP fragmentation with UDP

How we track TLSA names

Actively probe (.com&.net)

- **DNSSEC signed zones**
- HTTPS: port ***443***
- SMTP: port ***587***, ***465***, ***25***

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

Alternative sources:
watching resolvers or web crawls

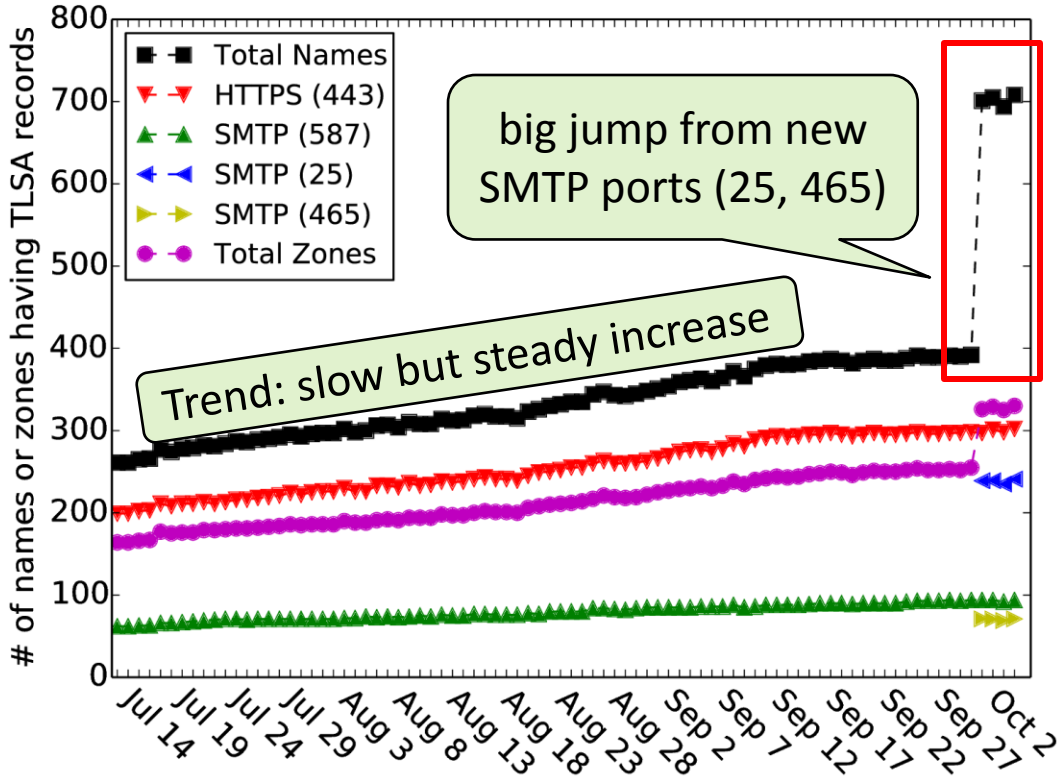
- But com and net are easy (in bulk) and provide better coverage

Findings and Observations

Understand the current TLSA use:

- How many TLSA names are there?
- Does DANE TLSA grow well?
- Is DANE TLSA used correctly?
- What are the most common TLSA parameters?
- Are TLSA replies problematically large?

The number of TLSA names



DANE TLSA use is early

- of the 461k signed zones, only about 708 TLSA names are found in the latest

DANE TLSA Penetration Rates

Penetration (P): each technology into its base of possible users
TLSA active zone: A zone contains at least one TLSA record

As of 2014-10-06:

zone	N_{all}	N_{dnssec}	N_{tlsa}	P_{dnssec} $(\frac{N_{dnssec}}{N_{all}})$	P_{tlsa} $(\frac{N_{tlsa}}{N_{dnssec}})$
com	114.7M	385k	136	.00336	.00035
net	15.1M	76k	140	.00507	.00183

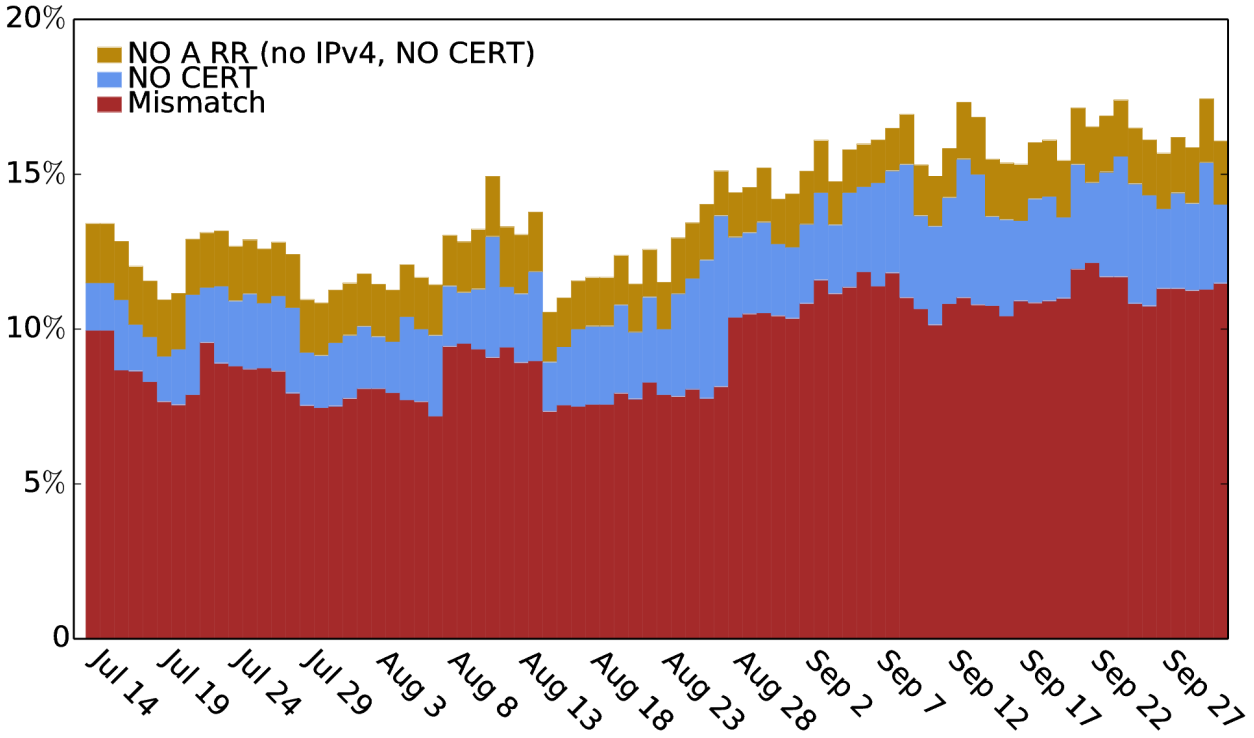
DANE TLSA: small but maybe off to a start, but still immature (2 years after standardization)

DNSSEC: deployment is still modest, 9 years after standardization (~3.5 years after signing .com and signing .net)

Is DANE TLSA used correctly

Validate TLSA records assuming DNSSEC integrity for simplicity

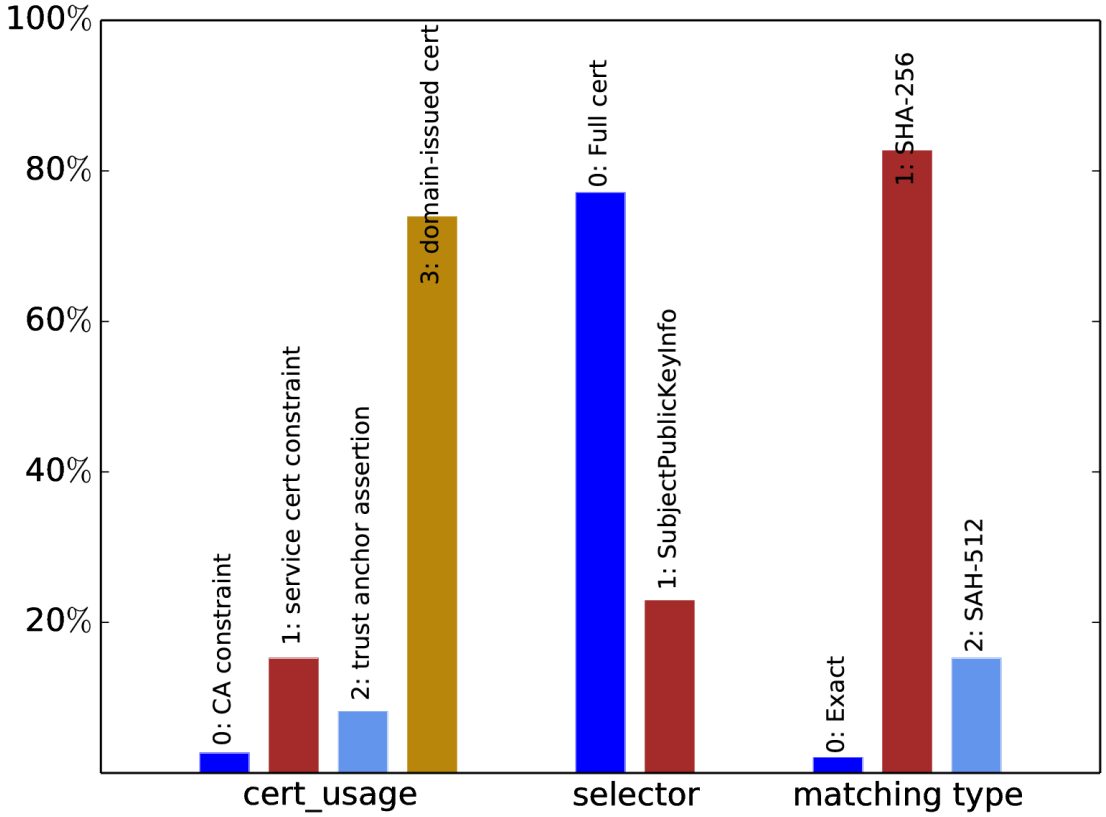
- No cert/No A record: DANE TLSA does not work even deployed
- Mismatch: the use of DANE TLSA will ***fail***



Consistently, 7%-12% TLSA records are mismatched

(ports 443 and 587 only)

Observed TLSA Parameters



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

SHA-256:
It is ***currently strong enough*** and not necessary to use stronger algorithm bringing more bits in DNS response

total 780 TLSA records in 701 TLSA responses captured on Oct. 2, 2014

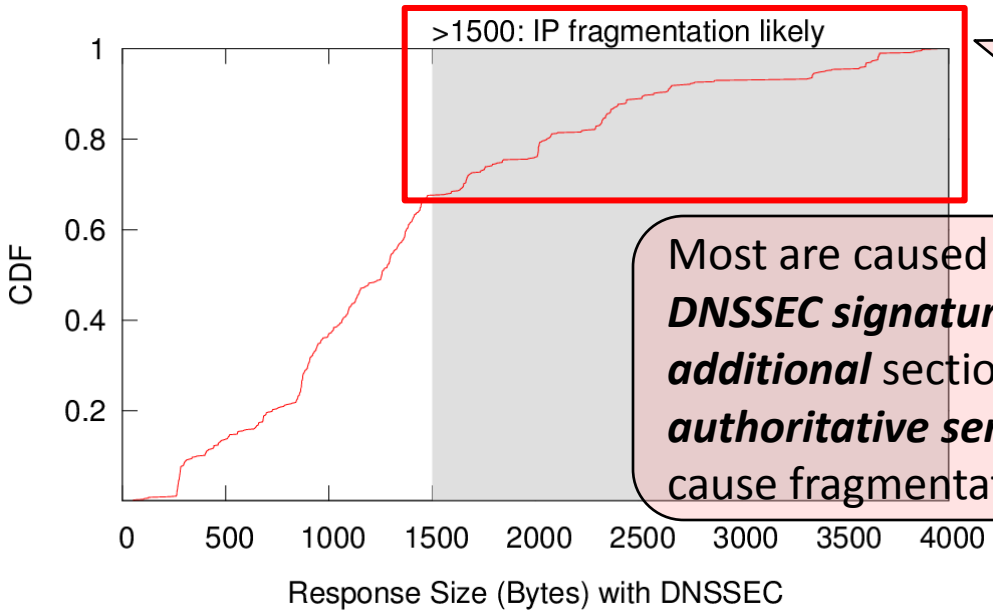
Problematically Large Responses

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

Query TLSA record with DNSSEC to authoritative servers of the 701 TLSA names on Oct. 2, 2014



31% TLSA responses with DNSSEC are larger than 1500 B

Most are caused by ***multiple RRs and DNSSEC signature*** in ***authority*** and ***additional*** sections. It provides ***more authoritative server options*** but may cause fragmentation problems

31% TLSA responses are Problematically Large

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

Conclusion

- We are tracking DANE growth
- We are working on improvements
  - IPv6 certificate validation
  - Check other RR types: OPENPGPKEY
- Data and code
  - working to get stats on the web and hope to release the code
- Early results:
  - DANE TLSA use is early, but growing
  - 7-12% of TLSA records are invalid
  - 31% replies force fragments
- We would like feedback from you