usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION
31ST USENIX SECURITY SYMPOSIUM

Under the Hood of DANE Mismanagement in SMTP

Hyeonmin Lee, Md. Ishtiaq Ashiq, Moritz Müller, Roland van Rijswijk-Deij, Taekyoung "Ted" Kwon, Taejoong Chung

Seoul National University, SIDN,
University of Twente & NLnet Labs, Virginia Tech

Key Findings

- DANE* is an Internet security protocol that is proposed to enable authentication of communication peers without relying on Certificate Authorities (CAs)

  *DNS-based Authentication of Named Entities (DANE)

Why?

30%

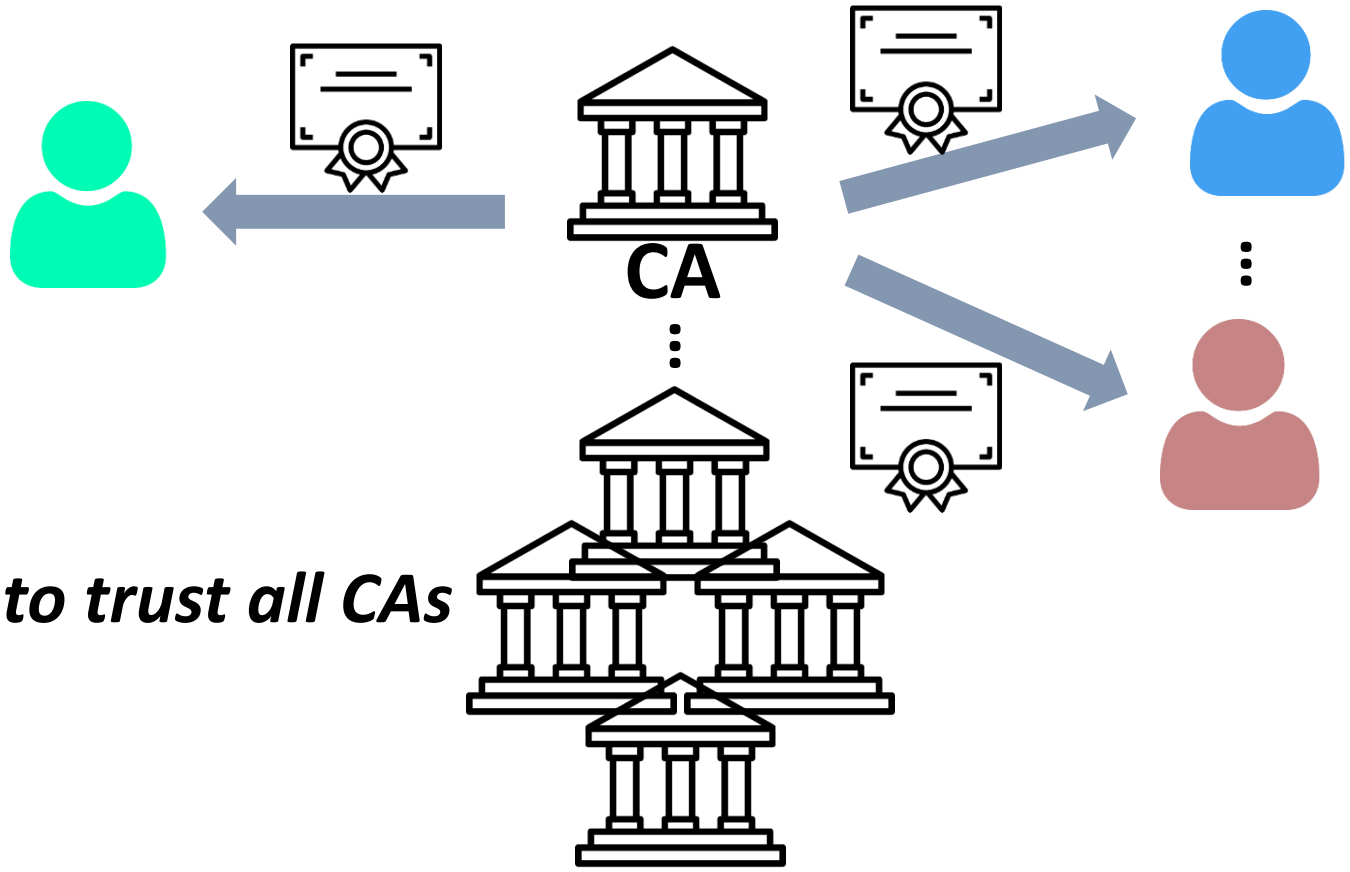
(self-hosted) SMTP servers managed by domain owners support DANE incorrectly

90%

SMTP servers Incorrectly rollover their keys

The Vulnerability in the CA-based PKI

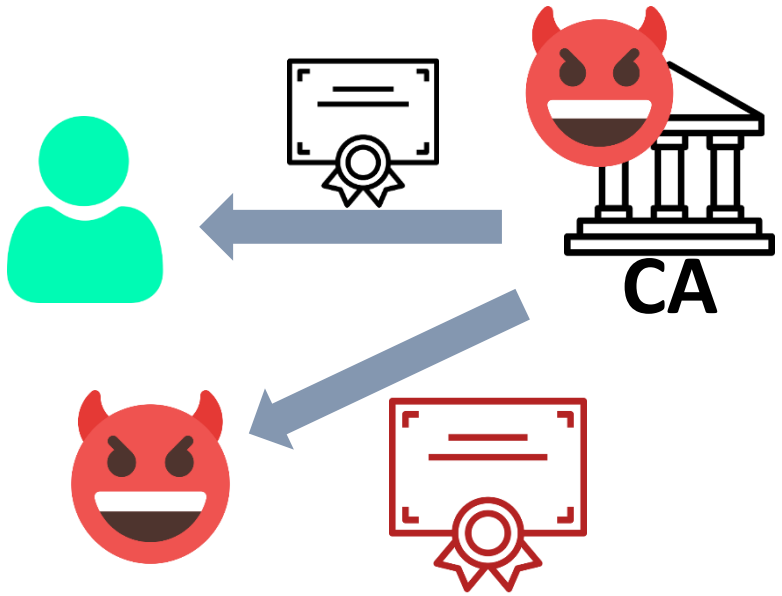
- In the current Public Key Infrastructure (PKI) model,
  - Certificates Authorities (CAs) can issue certificates ***to any domain name***



Need to trust all CAs

The Vulnerability in the CA-based PKI

- In the current Public Key Infrastructure (PKI) model,
  - Certificates Authorities (CAs) can issue certificates ***to any domain name***



[1]

Tech

Fake DigiNotar web certificate risk to Iranians

5 September 2011

[2]

Comodohacker: I can issue fake Windows updates

The hacker who breached security at DigiNotar and caused it to release fake digital certificates is now claiming he can exploit Microsoft's Windows Update to issue fake updates.

Lance Whitney Sept. 12, 2011 9:22 a.m. PT

- Several CAs were compromised and mis-issued fraudulent certificates

[1] BBC. (Sep 2011). “Fake DigiNotar web certificate risk to Iranians”
[2] Lance Whitney. CNET. (Sep 2011). “Comodohacker: I can issue fake Windows updates”

The Vulnerability in the CA-based PKI

- In the current Public Key Infrastructure (PKI) model,
  - Certificates Authorities (CAs) can issue certificates ***to any domain name***

Shook the faith in the PKI model

- Several CAs were compromised and mis-issued fraudulent certificates

[1] BBC. (Sep 2011). “Fake DigiNotar web certificate risk to Iranians”
[2] Lance Whitney. CNET. (Sep 2011). “Comodohacker: I can issue fake Windows updates”

The Vulnerability in the CA-based PKI

- Mitigations have been proposed

CT (Certificate Transparency)	DNS CAA (Certification Authority Authorization)
All certificates issued by CAs are **publicly logged** for monitoring	Domain name owners **specify CAs** that issue certificates for their domains

They still work based on CAs..

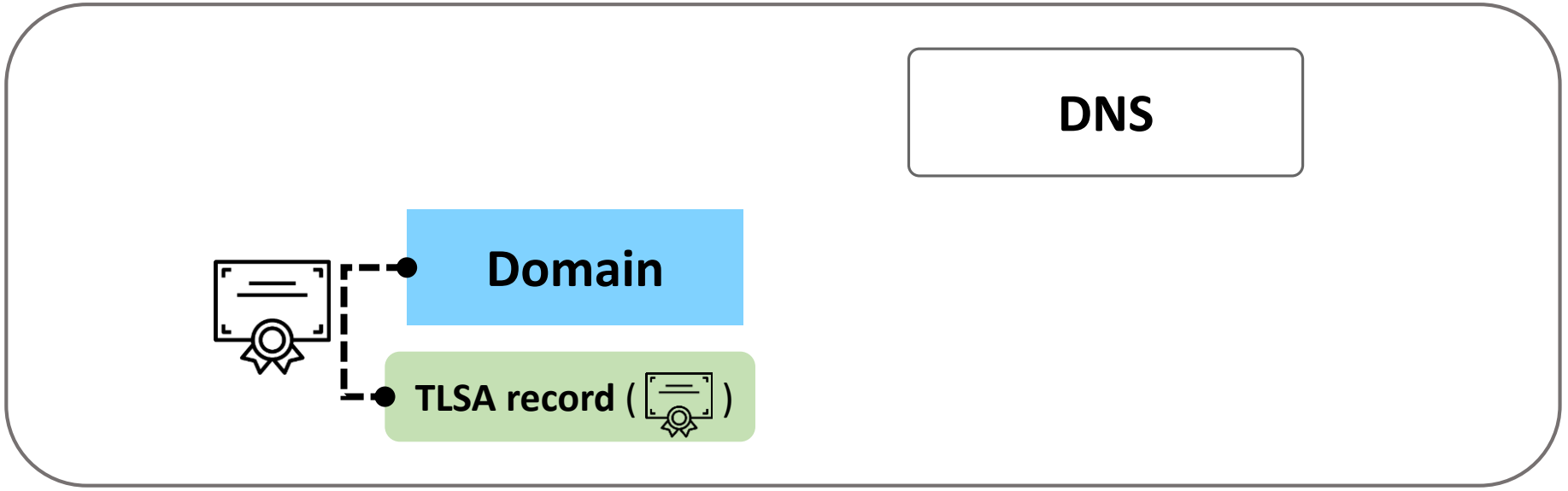
DNS-based Authentication of Named Entities (DANE)

[RFC 6698]
The DNS-Based Authentication of Name Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, Aug 2012

DNA-Based Authentication of Named Entities (DANE)

- DANE has been proposed to **bind certificates (public keys) to domain names without relying on CAs**

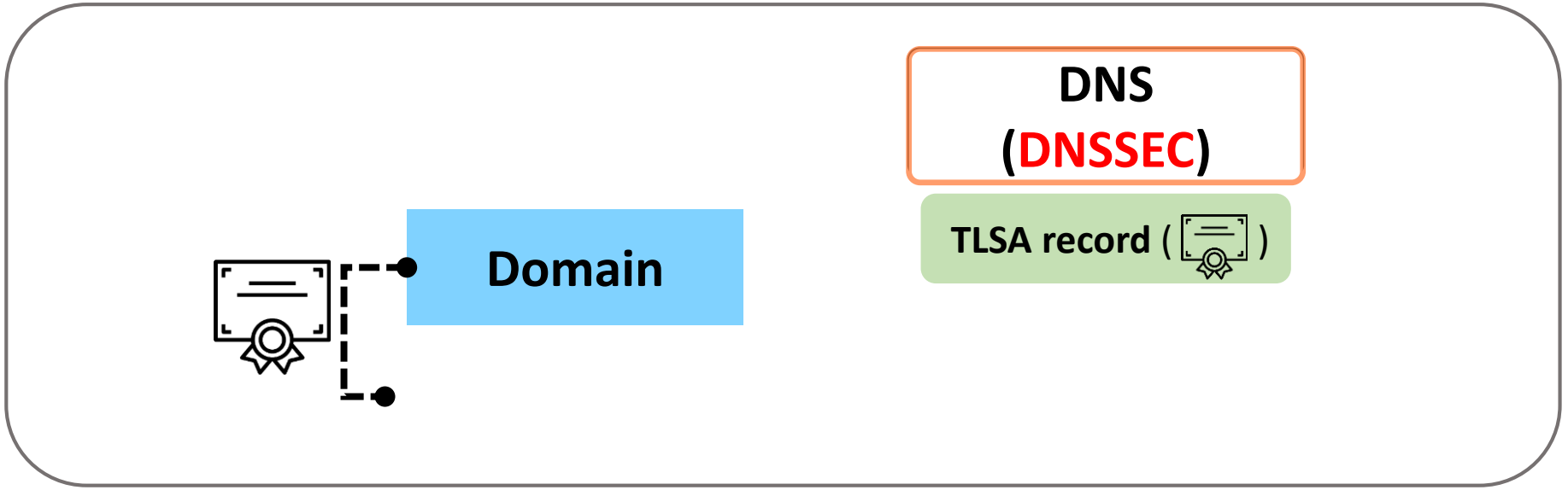
- How?
  - A domain publishes its certificate information as a DNS record **TLSA record**



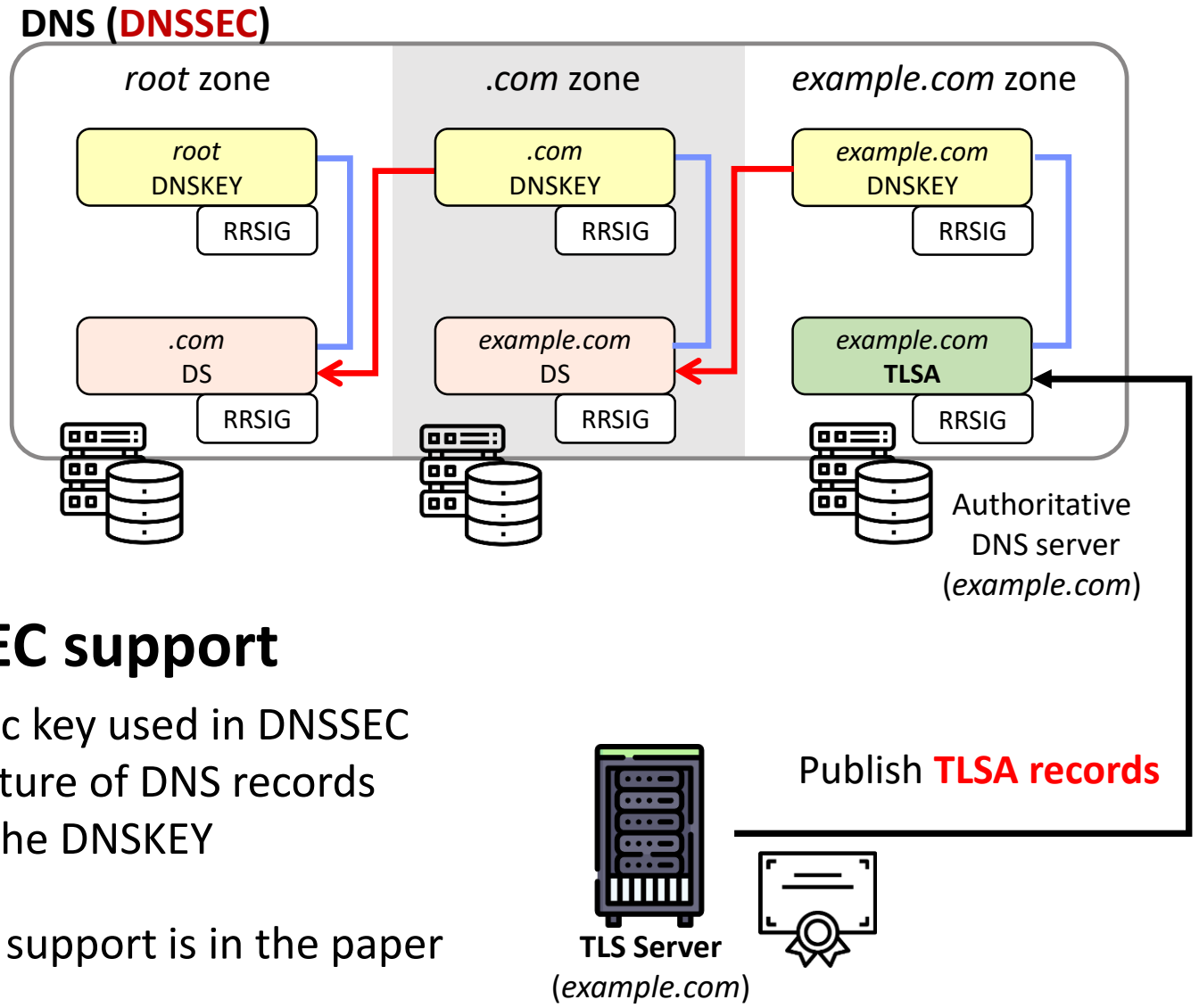
DNA-Based Authentication of Named Entities (DANE)

- DANE has been proposed to **bind certificates (public keys) to domain names without relying on CAs**

- How?
  - A domain publishes its certificate information as a DNS record **TLSA record**
  - A domain has to support **Domain Name System Security Extensions (DNSSEC)** to guarantee the integrity of **TLSA record**



How to deploy DANE?

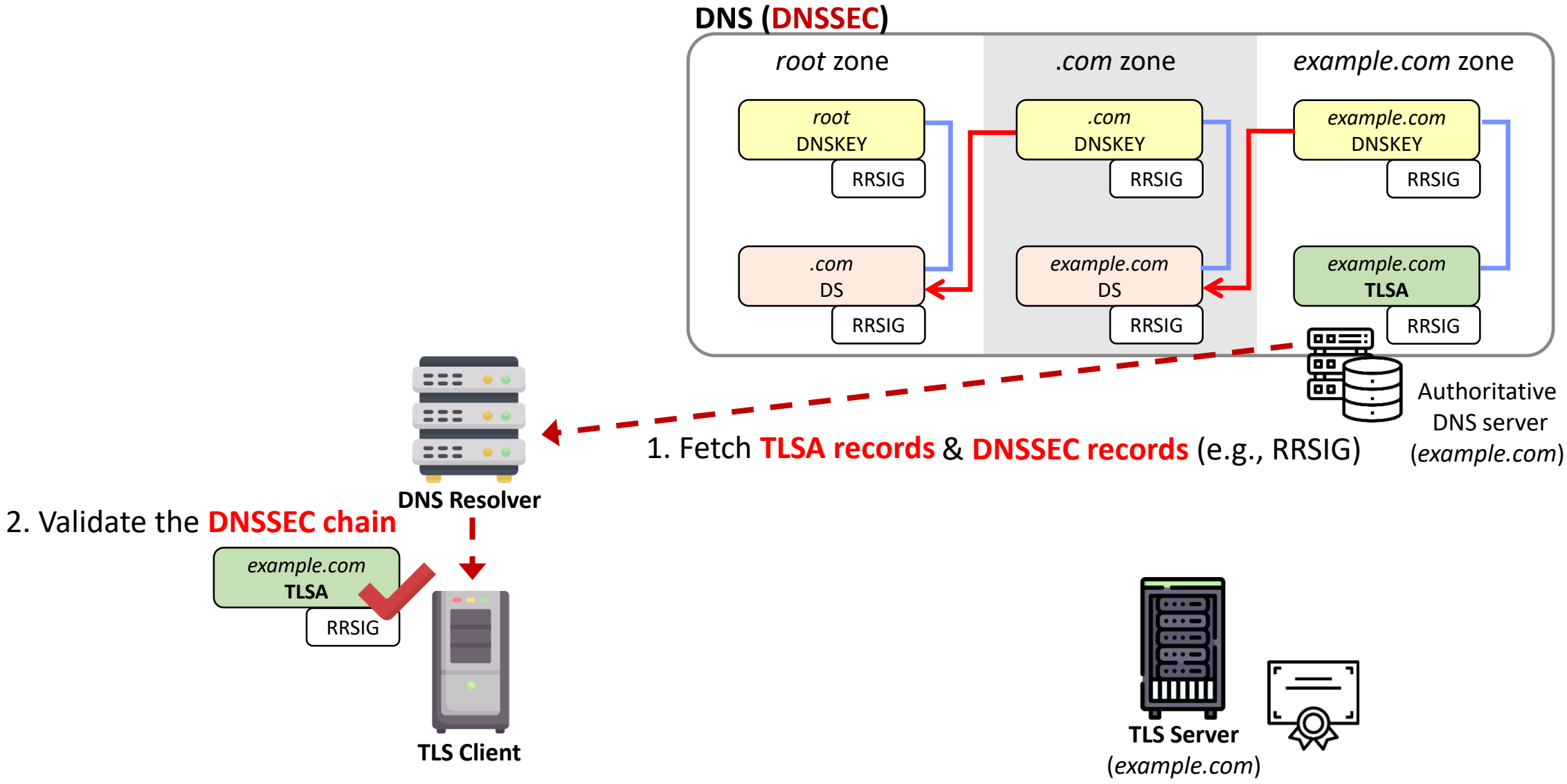


Necessary: DNSSEC support

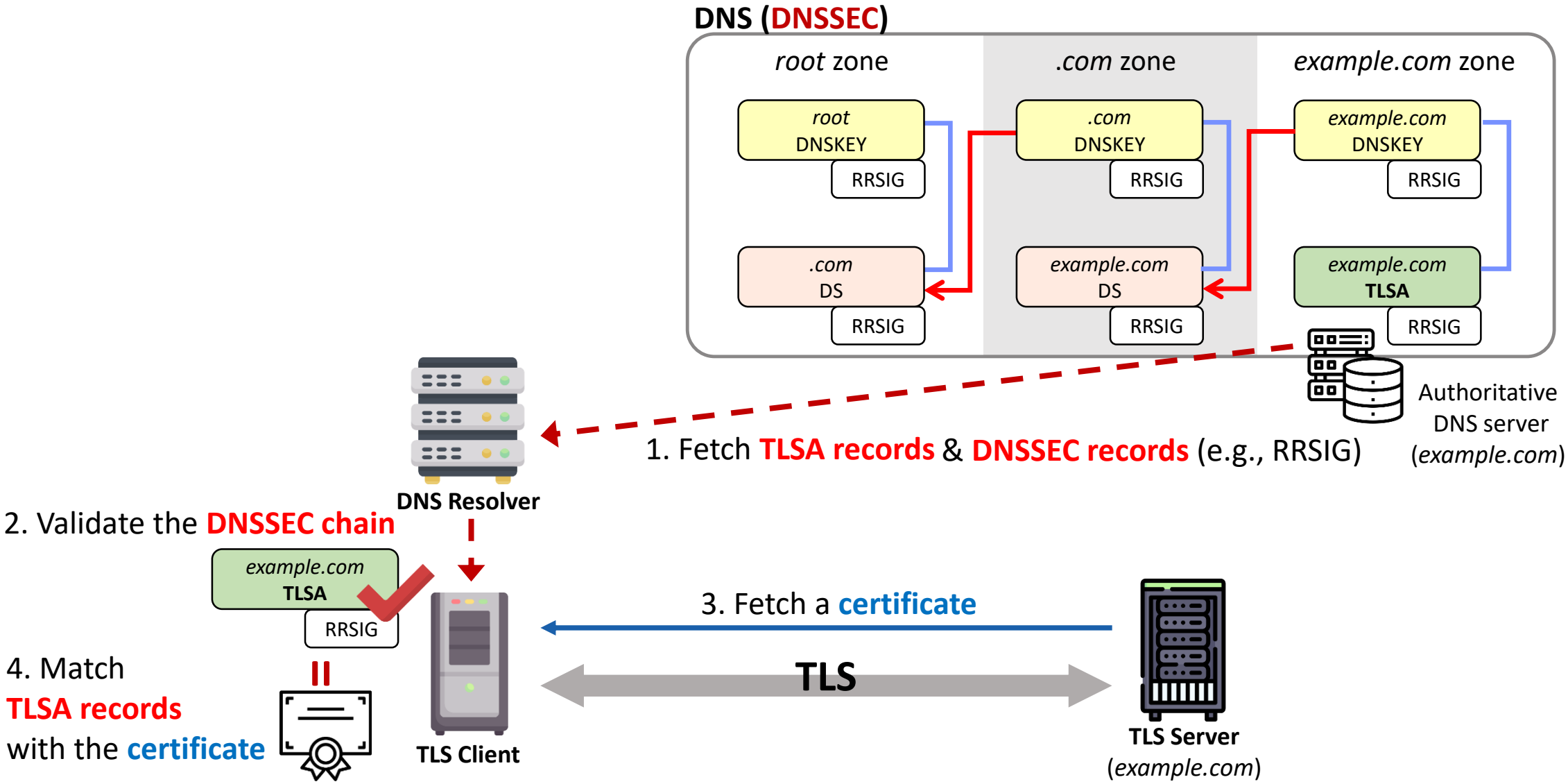
- **DNSKEY** record: public key used in DNSSEC
- **RRSIG** record: a signature of DNS records
- **DS** record: a hash of the DNSKEY

*More information about DNSSEC support is in the paper

DANE Validation Process

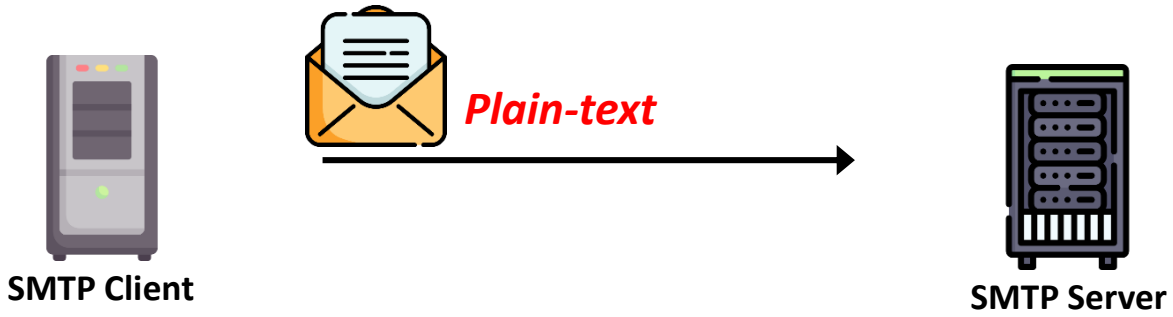


DANE Validation Process



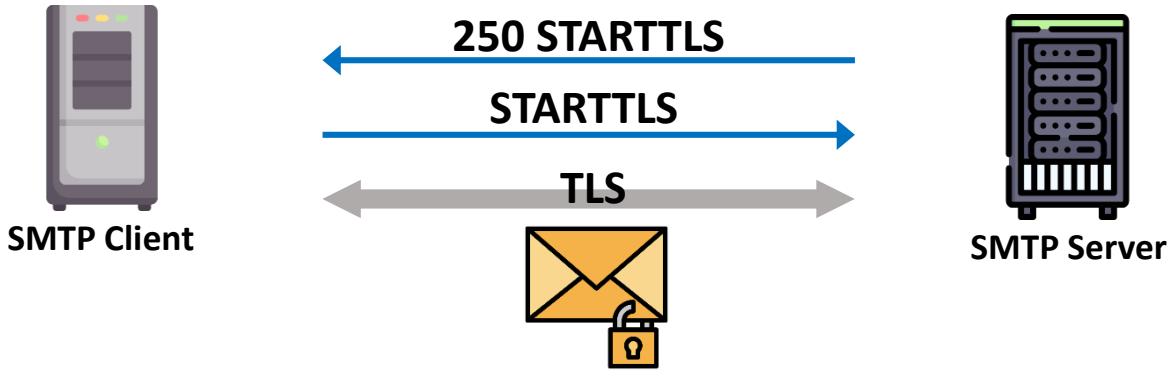
DANE and SMTP

- **Simple Mail Transfer Protocol (SMTP)** is a communication protocol for electronic mail transmission
  → **No security features** in its initial design



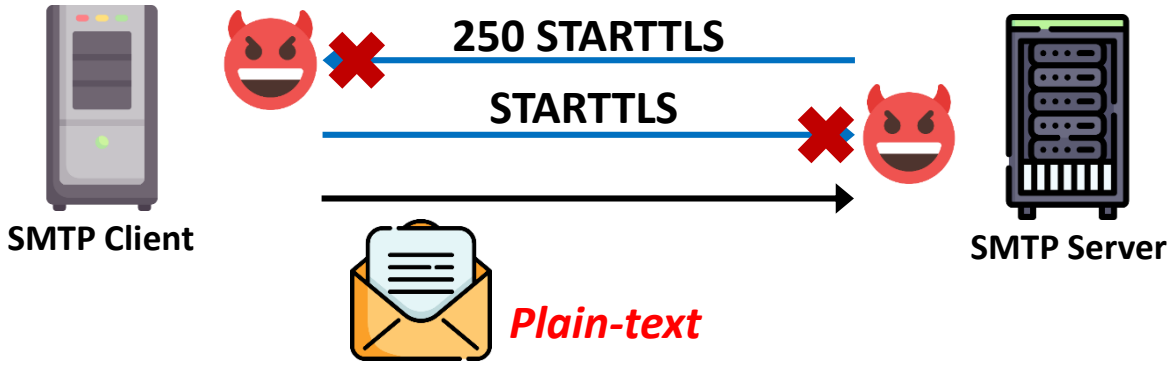
DANE and SMTP

- **Simple Mail Transfer Protocol (SMTP)** is a communication protocol for electronic mail transmission
  - → **No security features** in its initial design
  - → **STARTTLS** is used to support opportunistic TLS



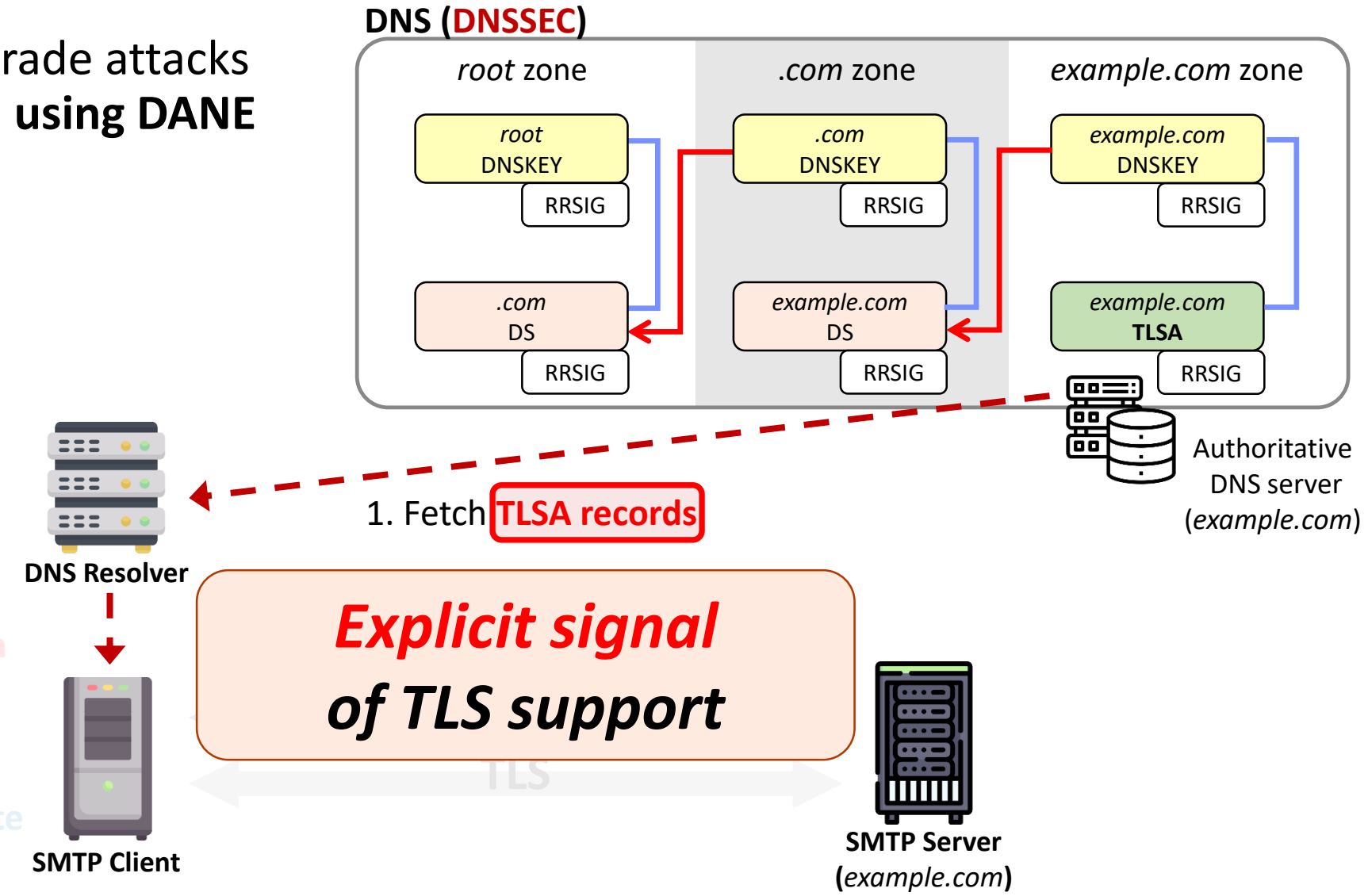
DANE and SMTP

- **Simple Mail Transfer Protocol (SMTP)** is a communication protocol for electronic mail transmission
  - → **No security features** in its initial design
  - → **STARTTLS** is used to support opportunistic TLS
  - → **STARTTLS** is vulnerable to **downgrade attacks**



DANE and SMTP

- STARTTLS downgrade attacks can be **mitigated using DANE**

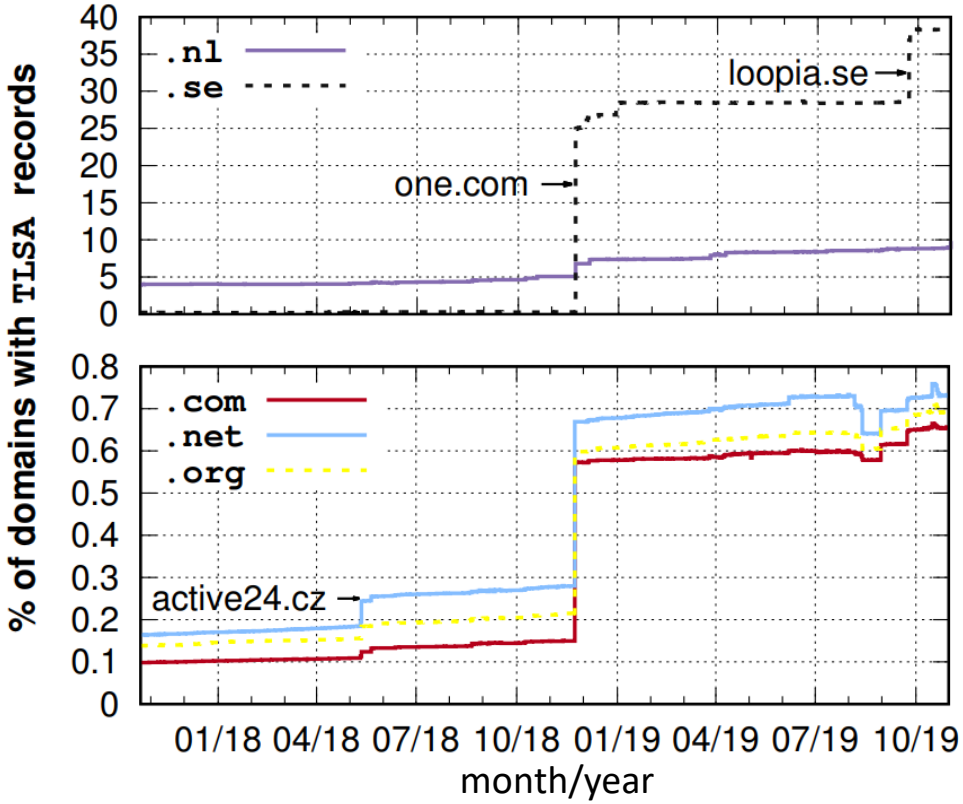


How DANE is Deployed?

- Our previous work on *USENIX Security 2020*
  - Lee et al. "*A Longitudinal and comprehensive Study of the DANE Ecosystem in Email*"
  - Scan TLSA, MX records for 2 years (Oct 2017 ~ Oct 2019)

- The deployment rate is low.. but ***increasing***!

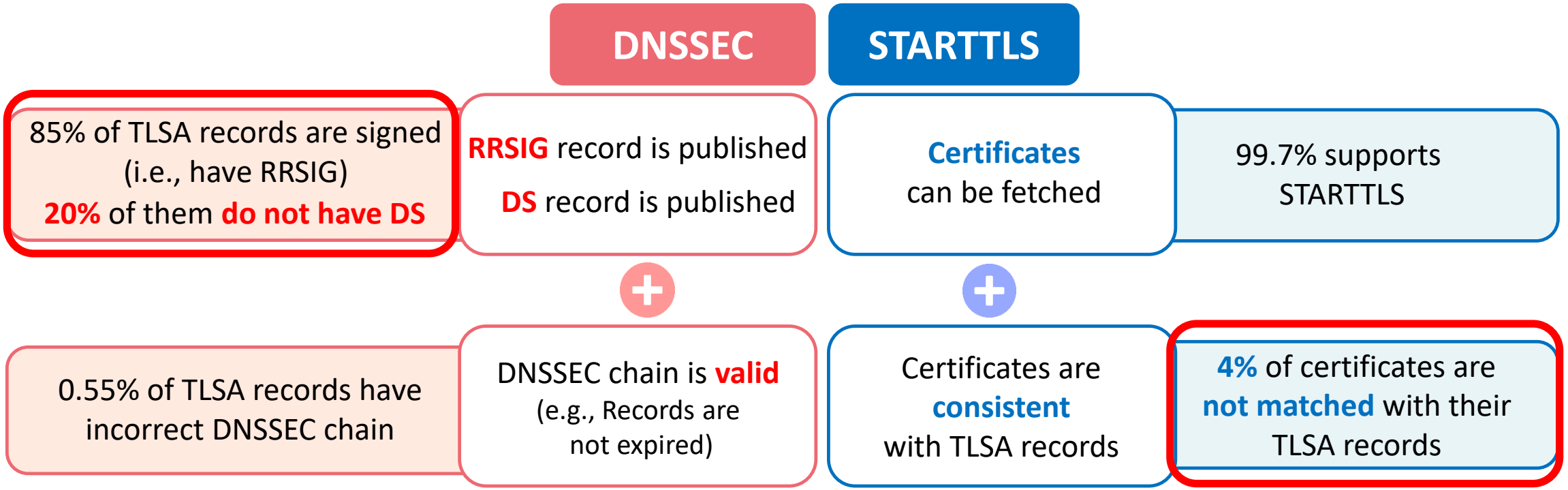
- **.nl** and **.se** show high deployment
  → Due to financial incentives from registries



How DANE is Deployed?

- Are they correct?

*Lee et al. *"A Longitudinal and comprehensive Study of the DANE Ecosystem in Email"*, USENIX Security '20



Why?

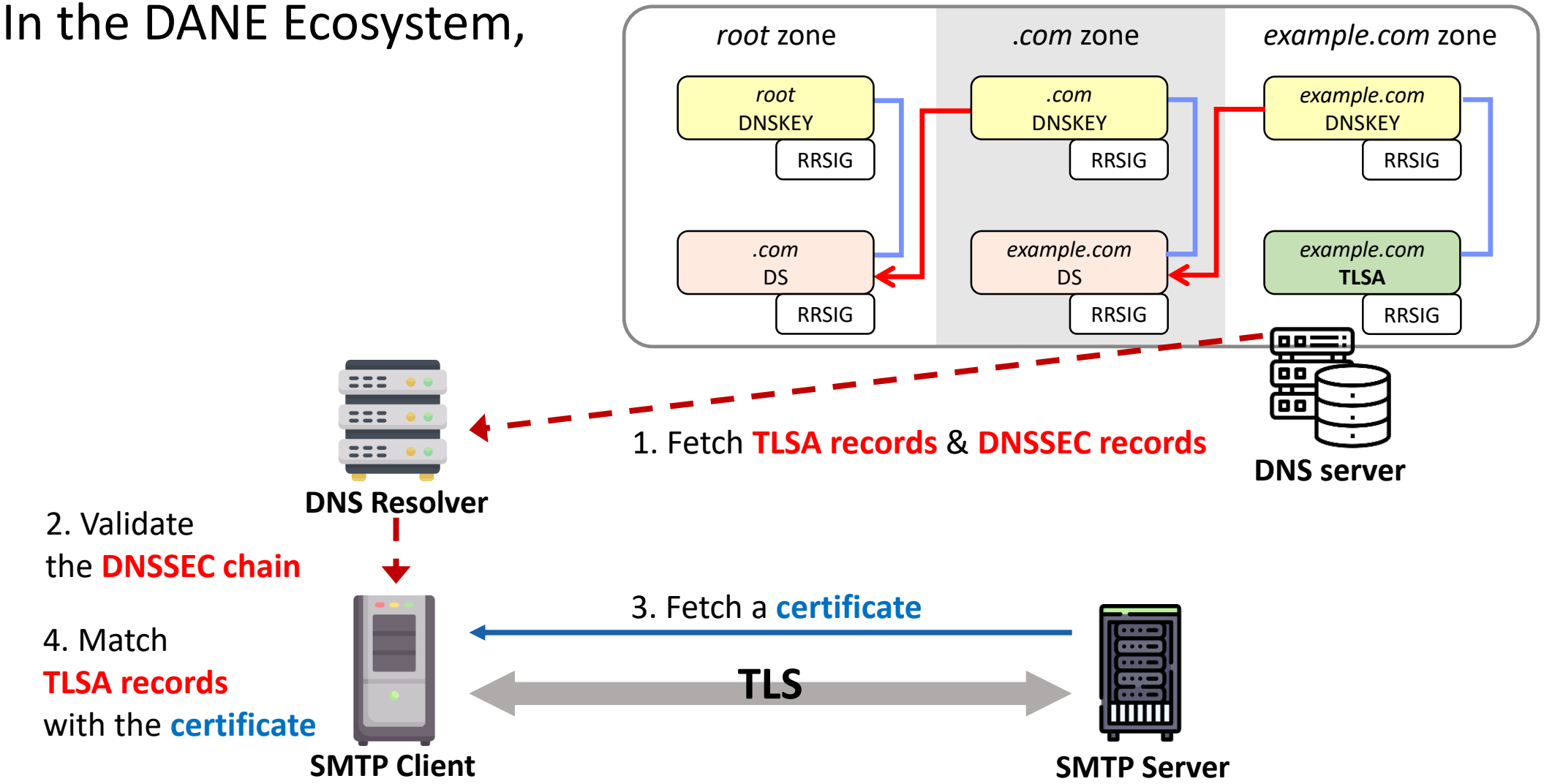
→ Motivation of our USENIX Security '22 paper

Why do domains fail to support DANE correctly?

- USENIX Security 2022 -

Entities in DANE Management

In the DANE Ecosystem,



Entities in DANE Management

In the DANE Ecosystem,

Each server can be self-hosted or outsourced

Self-hosted

Domain administrators manage
DNS servers and **SMTP servers** coherently **by themselves**

Outsourced

Domain administrators **outsource**
DNS servers or **SMTP servers**

Entities in DANE Management

Q. The quality of DANE management can be different *depending on "who" manages server*?

Each server can be self-hosted or outsourced

Self-hosted

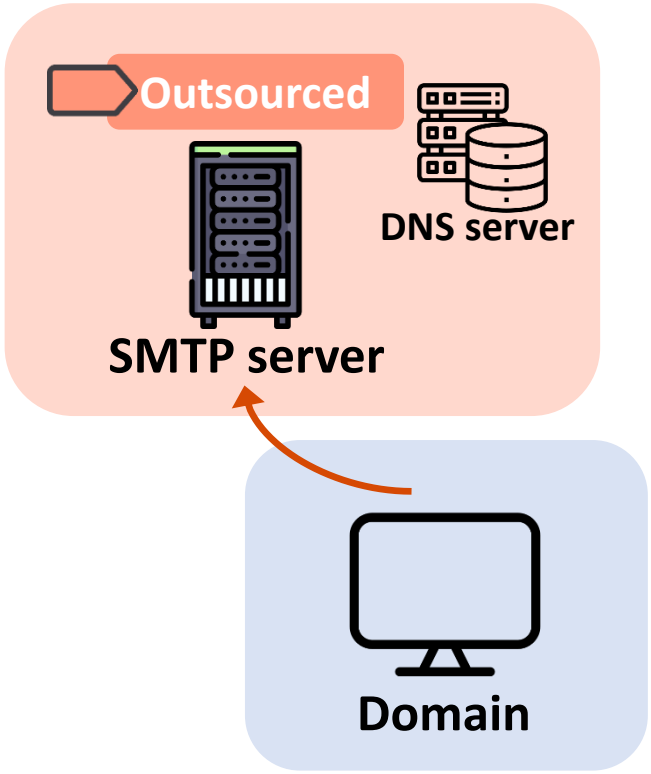
Domain administrators manage
DNS servers and **SMTP servers** coherently **by themselves**

Outsourced

Domain administrators **outsource**
DNS servers or **SMTP servers**

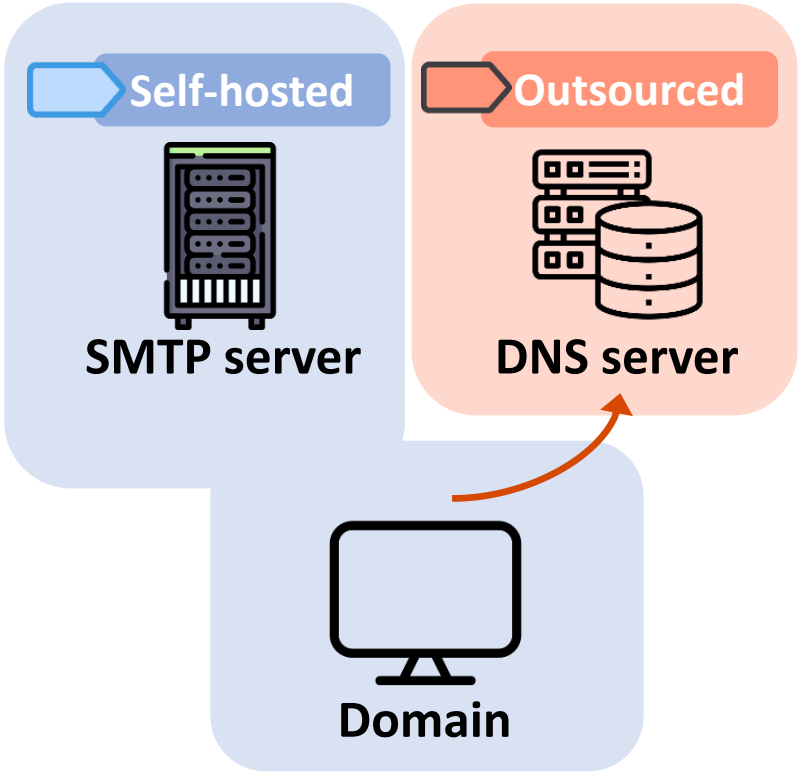
Managing Case Classification

- 3 cases of DANE management



SMTP server
Outsourcing

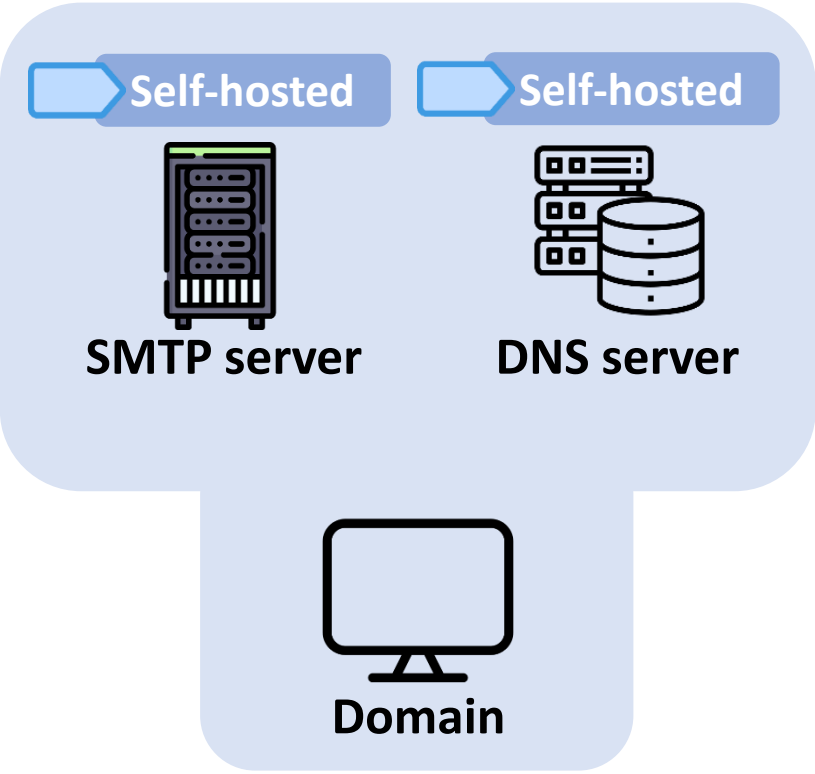
[SO case]



SMTP server
Self-hosting

DNS server
Outsourcing

[SSDO case]

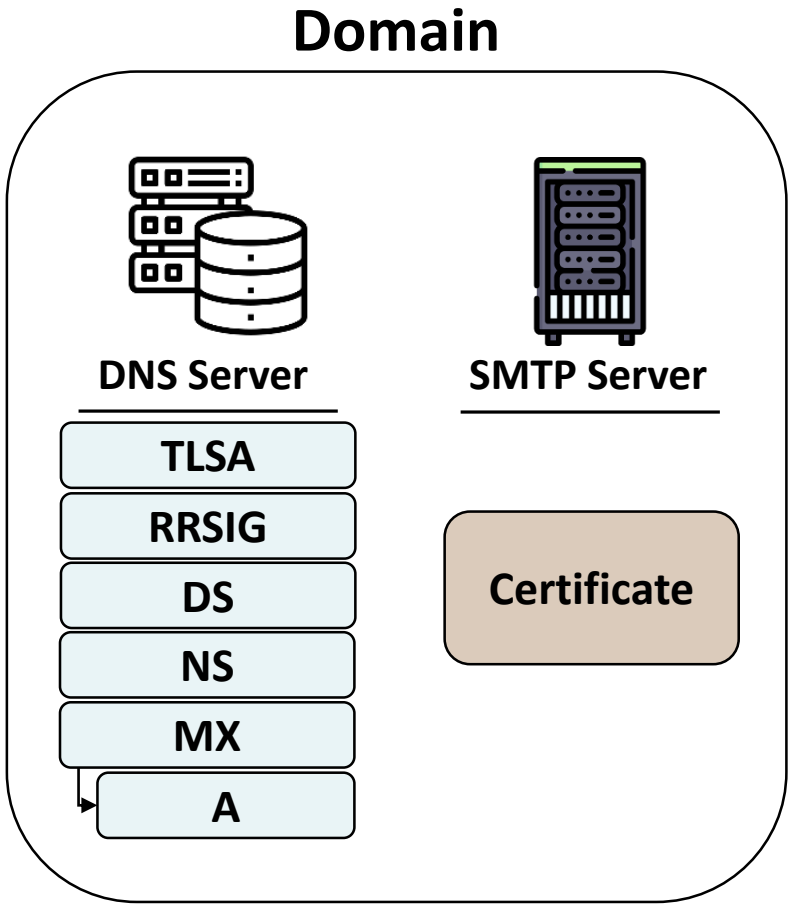


SMTP server
Self-hosting

DNS server
Self-hosting

[SSDS case]

Dataset



All second-level domains under
.com*, *.net*, *.org*,** and ***.se

July 2019 ~ February 2021
Daily and Hourly scan

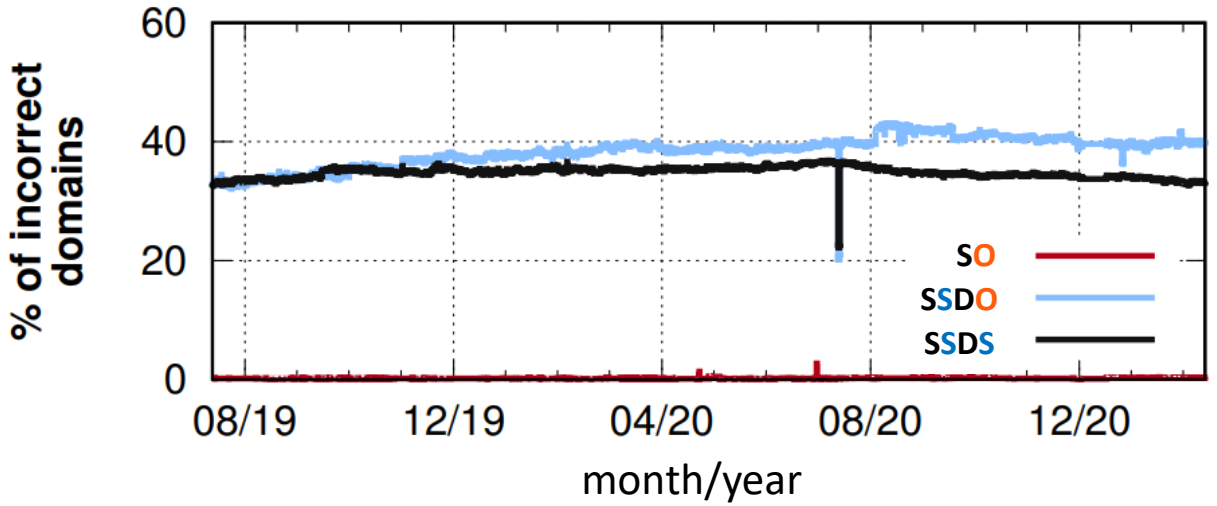
*Details of methodology for determining managing entities are in the paper

Managing Entities and Management Qualities

- The ratios of domains that support DANE incorrectly in **SSDO, SSDS are much higher than SO**

Self-hosting SMTP servers are more error-prone

Let's focus on SMTP Self-hosting cases (SSDO and SSDS)



*SO: SMTP Outsourcing
SSDO: SMTP Self-hosting, DNS Outsourcing
SSDS: SMTP Self-hosting, DNS Self-hosting

Why TLSA Validations Fail?

- 2 failure reasons: (1) **DNSSEC failure** & (2) **Mismatch of certificates and TLSA records**

DNSSEC Failure

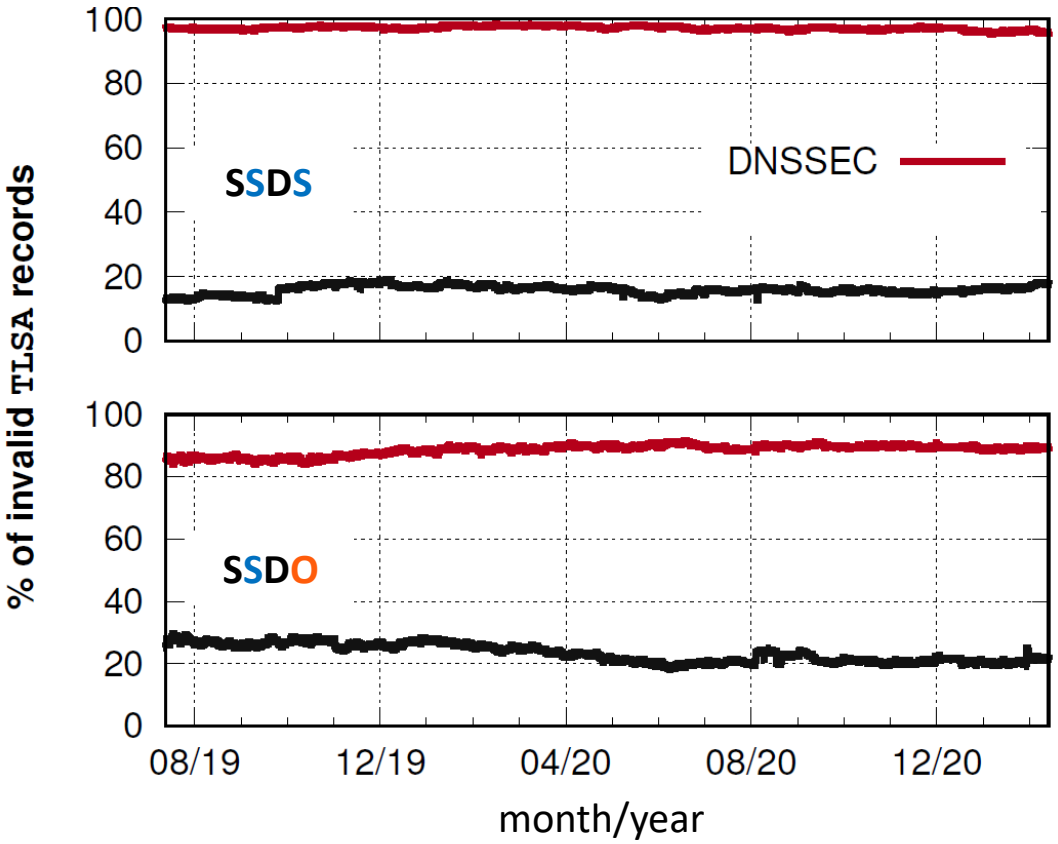
- The **dominant reason** of validation failures

  →99% of DNSSEC failures are due to **missing DS records**

Mismatch

- 16~23% of SMTP servers have certificates that are not matched with their TLSA records

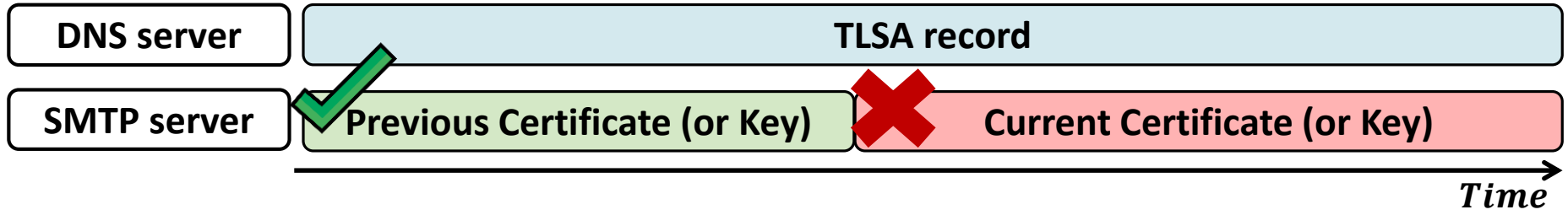
Why?



*SSDO: SMTP Self-hosting, DNS Outsourcing
SSDS: SMTP Self-hosting, DNS Self-hosting

Why Mismatches Happen?

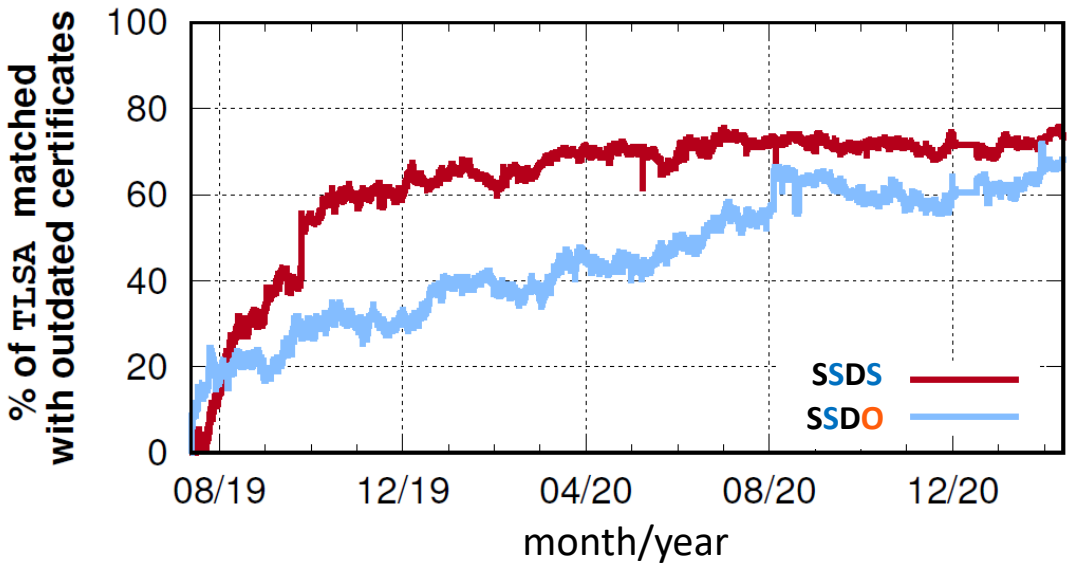
- Are the mismatched TLSA records valid before?
  - Checked the percentage of TLSA records that are mismatched with certificates at the time of the scan, but can be matched with certificates used before



- The percentage increases continuously

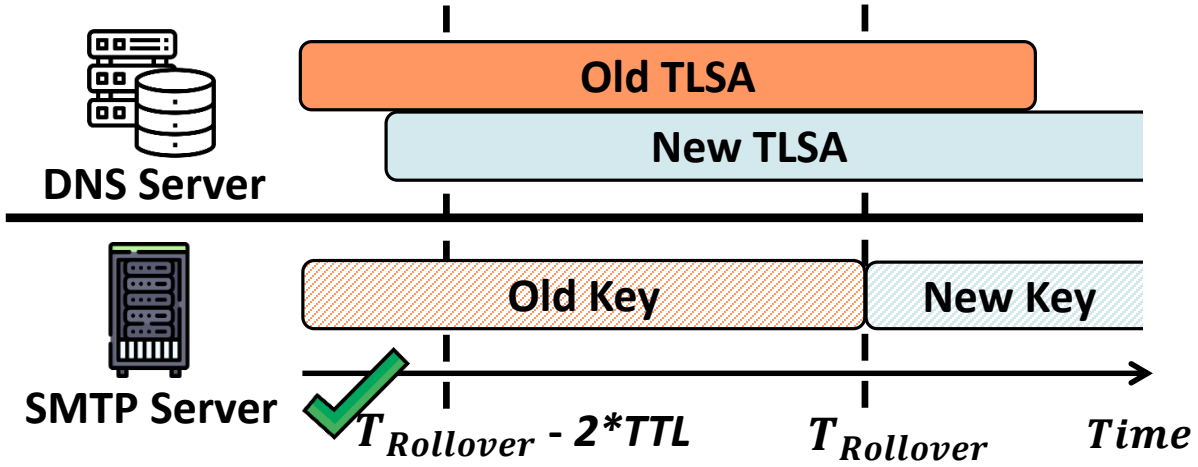
→**Certificates are changed but the corresponding TLSA records are not updated timely**

Incorrect Key Rollover



DANE Key Rollover

- **Key rollover**? Update of public and private key pairs
- **Correct** key rollover?
  → An SMTP server must **publish the new TLSA record** to a DNS server **in advance**, at least 2 TTLs before (to consider DNS cache)



Case	SMTP servers		Domains	
	Total	Incorrect Rollover	Total	Incorrect Rollover
SO	277	255 (92%)	54,052	34,056 (63%)
SSDO	275	240 (87%)	278	242 (87%)
SSDS	594	544 (92%)	585	546 (93%)

90% of SMTP servers conduct rollovers incorrectly

Why Servers Conduct Rollovers..?

Actually, DANE does not require a key rollover
when using *DANE-TA* or *DANE-EE* usages - DANE RFC
(99% of SMTP servers use *DANE-TA* or *DANE-EE)*

In our data

Automated CAs

87% of certificates are issued by *Let's Encrypt* and *Sectigo*

Is there any problem?

Side effect

Enforce key rollovers..

Incorrect Rollovers and Let's Encrypt

- *DANE-TA* usage allows domains publish ***TA's certificate** as a TLSA record
  - Usually, TA's certificate is not changed often (compared to leaf certificates)

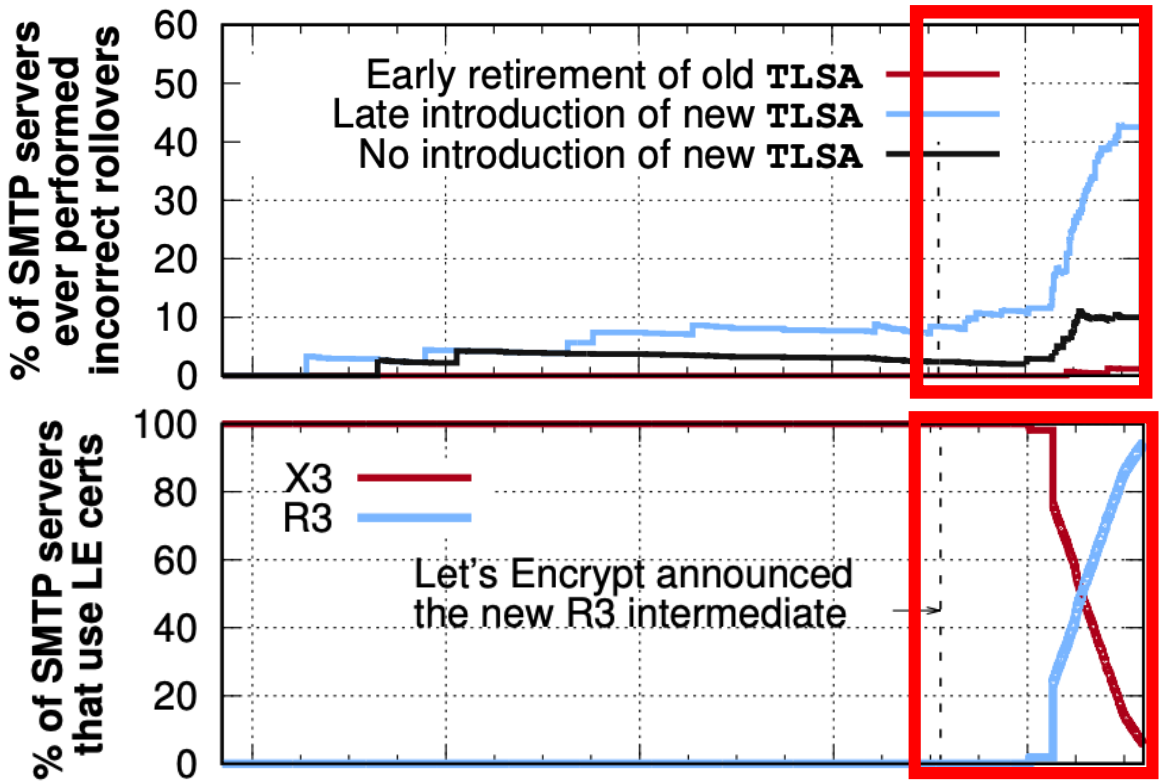
*TA: Trust Anchor

1. Incorrect rollover ratios are **lower than other usages** when using *DANE-TA*

2. The **explosion** from October 2020

   →***Let's Encrypt (LE)* introduced the new intermediate certificate** (from X3 to R3)

   →SMTP servers **failed to respond properly**; do not rollover their TLSA records correctly



Conclusion

- Investigated *why* domains fail to manage DANE correctly

- Revealed reasons for mismanagement
  1) DNSSEC issues: *missing DS records* in parent zones
  2) Mismatches of TLSA and certificates: key changes due to *automatic certificate reissuance* of CAs

- Other findings – *please refer our paper*
  - Confirmed that SMTP servers use CA-issued certificates to consider *compatibility* with others
  - Implemented an automatic key rollover script to support DANE management

[Datasets & source code]

- https://dane-study.github.io/

Thank you!

Any questions?

Hyeonmin Lee
min0921110@gmail.com