ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

SLAC 2024

Why TLS is better without STARTTLS:

A Security Analysis of STARTTLS in the Email Context

Fabian Ising[1], Damian Poddebniak[2], Hanno Böck[2], Sebastian Schinzel[1,3]

[1] Fraunhofer SIT | ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit

[2] Independent Researcher

[2] FH Münster

https://nostarttls.secvuln.info/

$ whoami

Dr.-Ing. Fabian Ising

- Wissenschaftlicher Mitarbeiter am Fraunhofer SIT
  - Abteilung: Applied Cryptography and Medical Security (ACM)
- Trainer im Lernlabor Cybersicherheit (LLCS)
  - Trainingsschwerpunkt: E-Mail-Sicherheit für Unternehmen

- Forschung:
  - Angewandte Kryptographie, insb. E-Mail-Sicherheit
  - Sicherheit von Netzwerkprotokollen

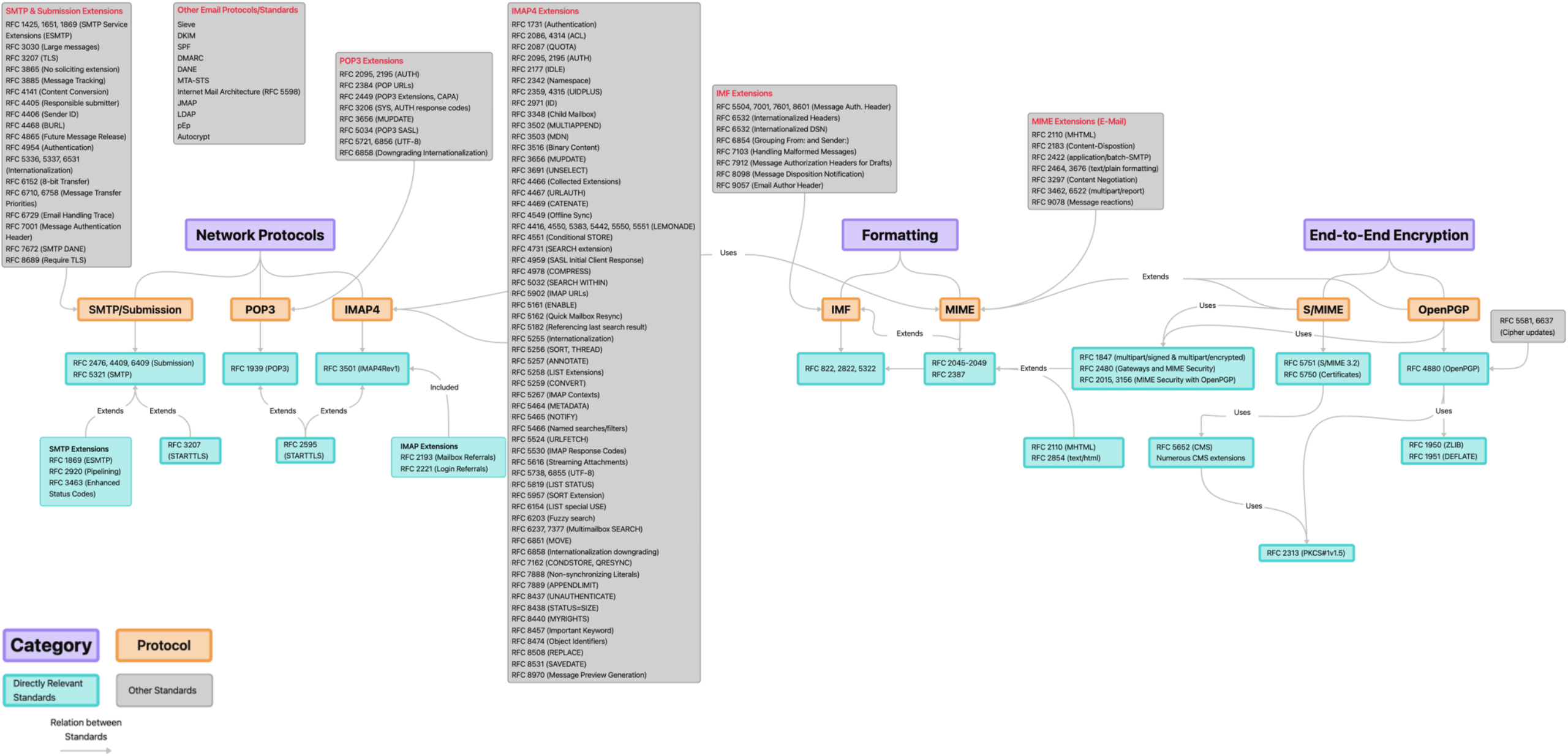
Lernlabor Cybersicherheit

Who are you?

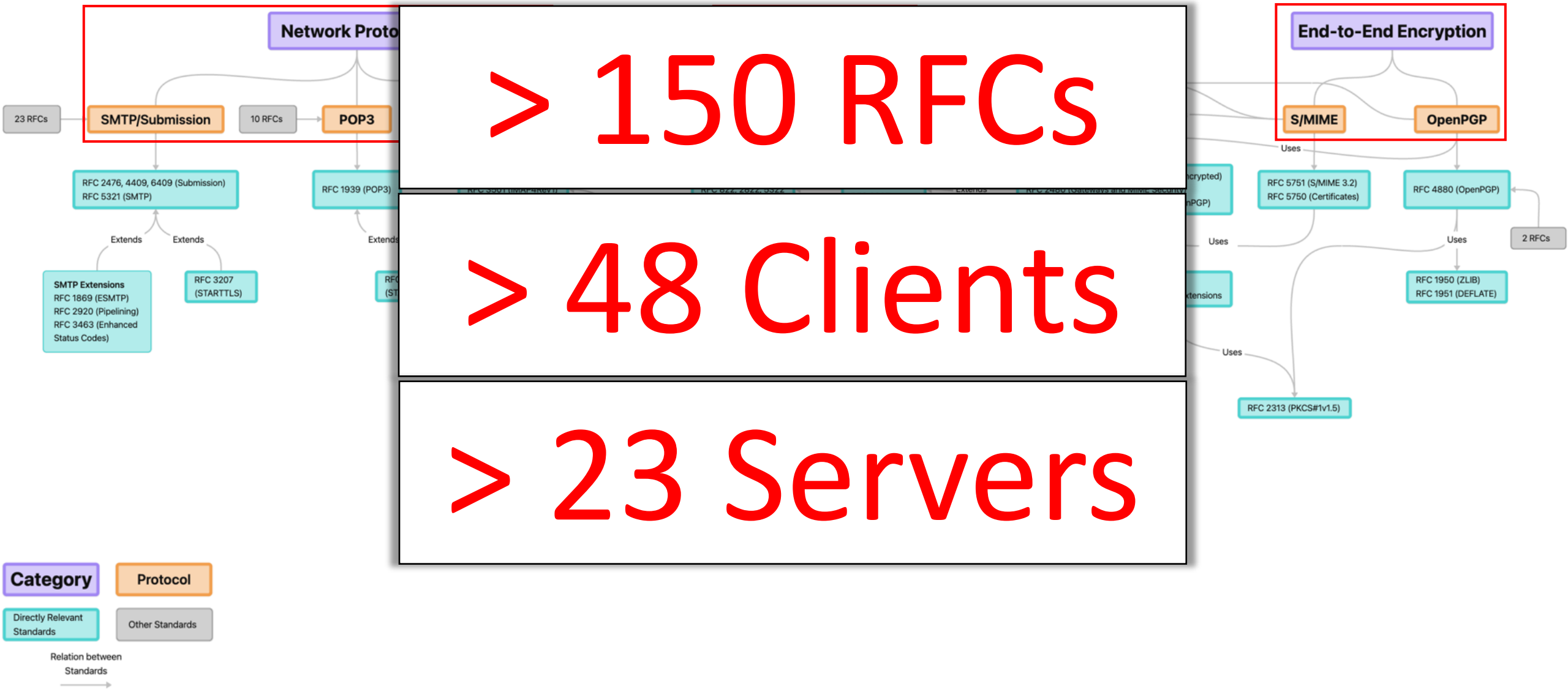
Wer von Ihnen betreut einen E-Mail-Server? (auch privat)

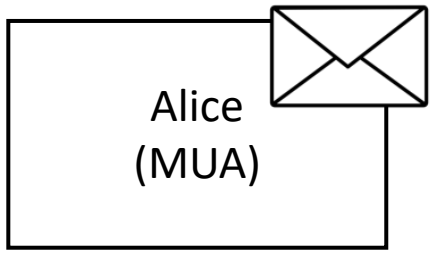
Wer von Ihnen entwickelt/wartet ein E-Mail-Software-Produkt?
(Server, Client, Gateway, ...)

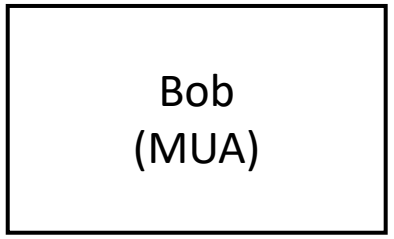
E-Mail “in a nutshell“



E-Mail “in a nutshell“

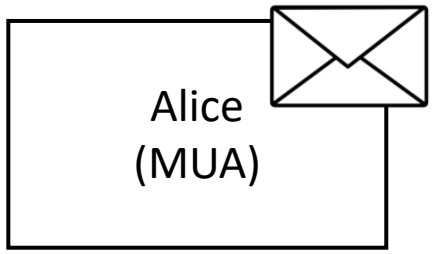



Alice
(MUA)


Bob
(MUA)

MSP

MSP

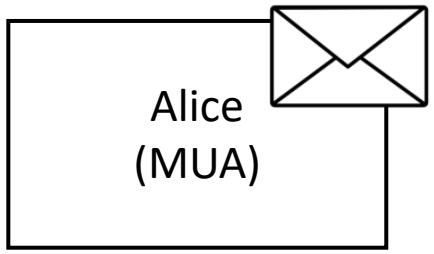


Bob
(MUA)

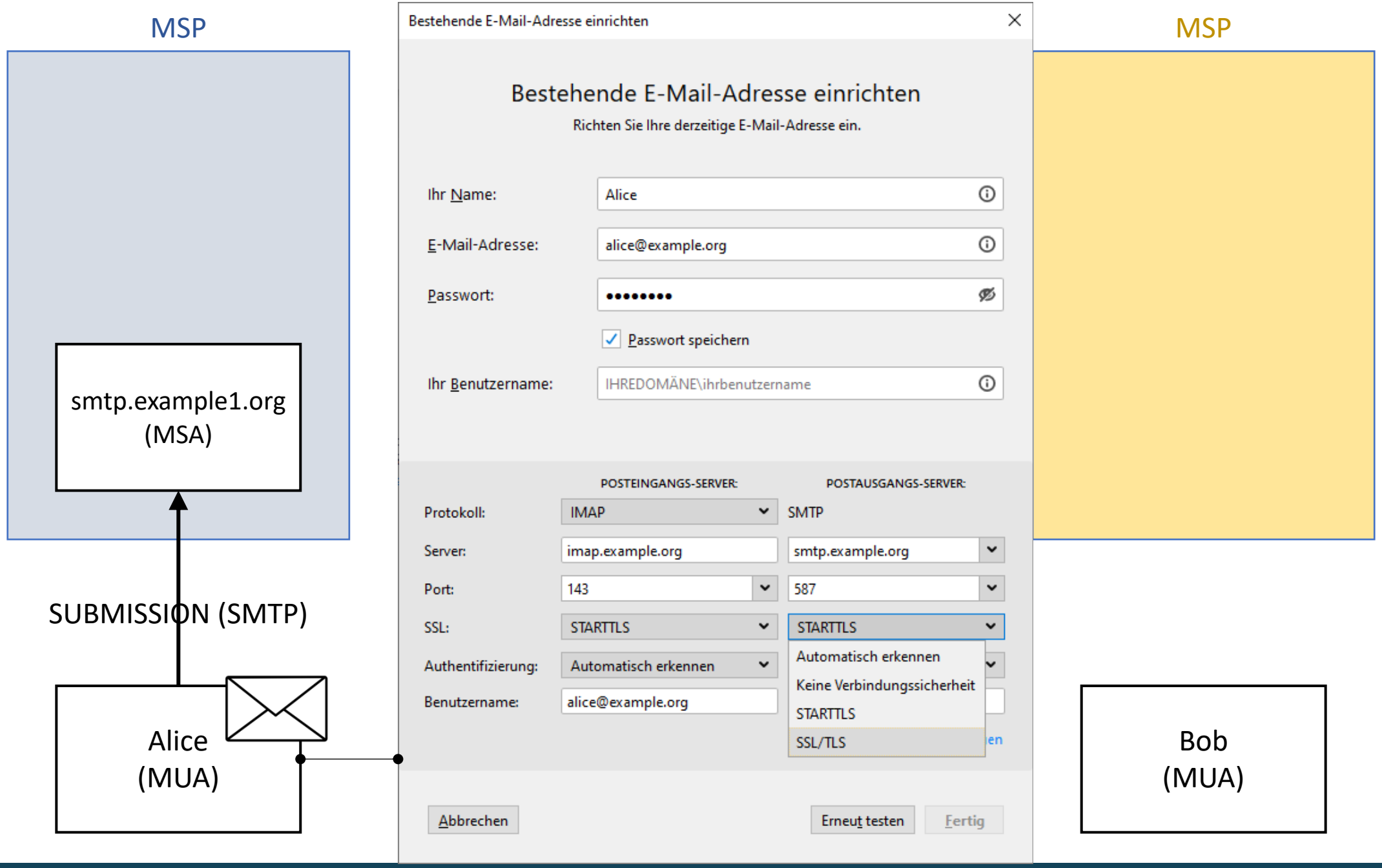
MSP

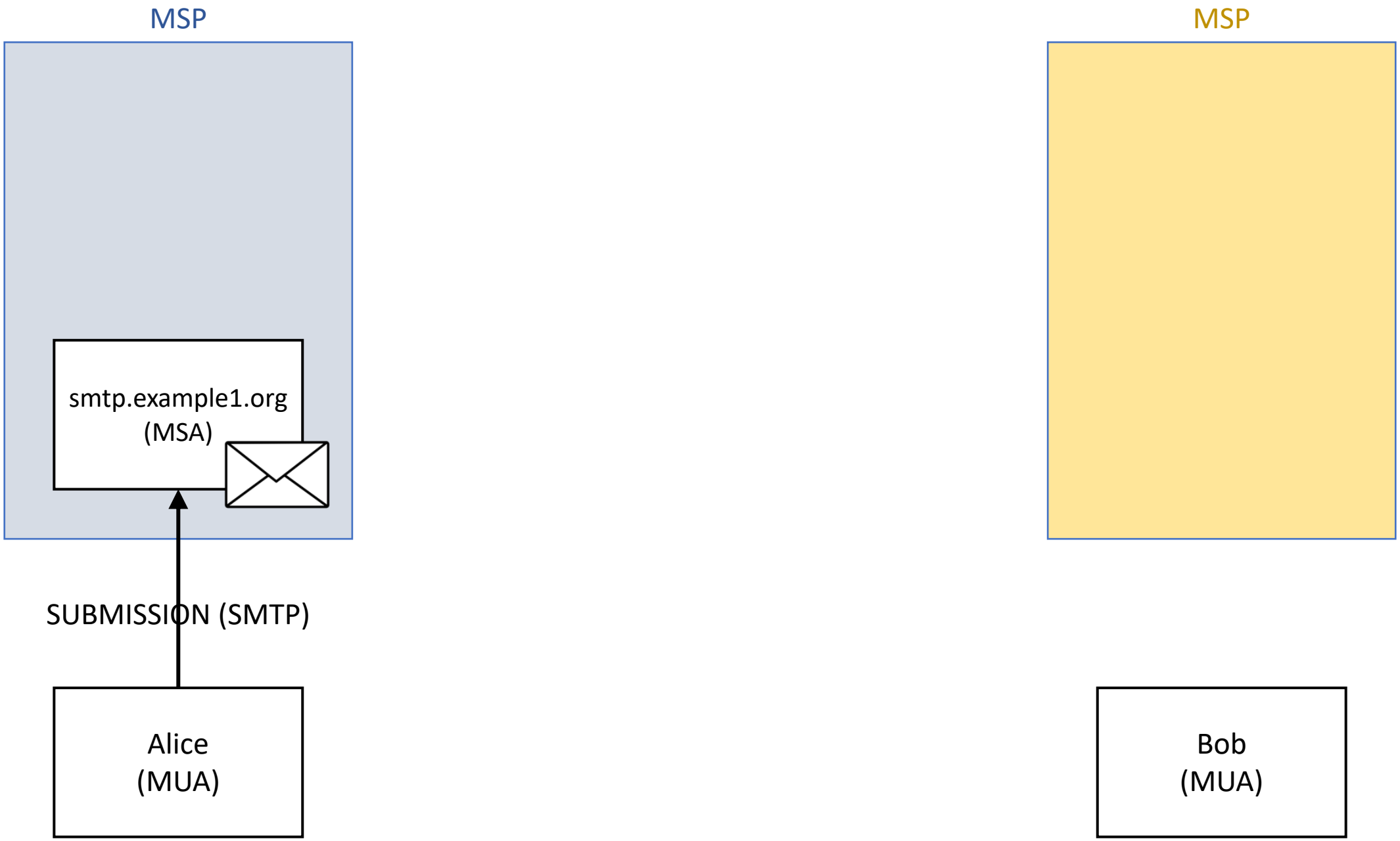
smtp.example1.org
(MSA)

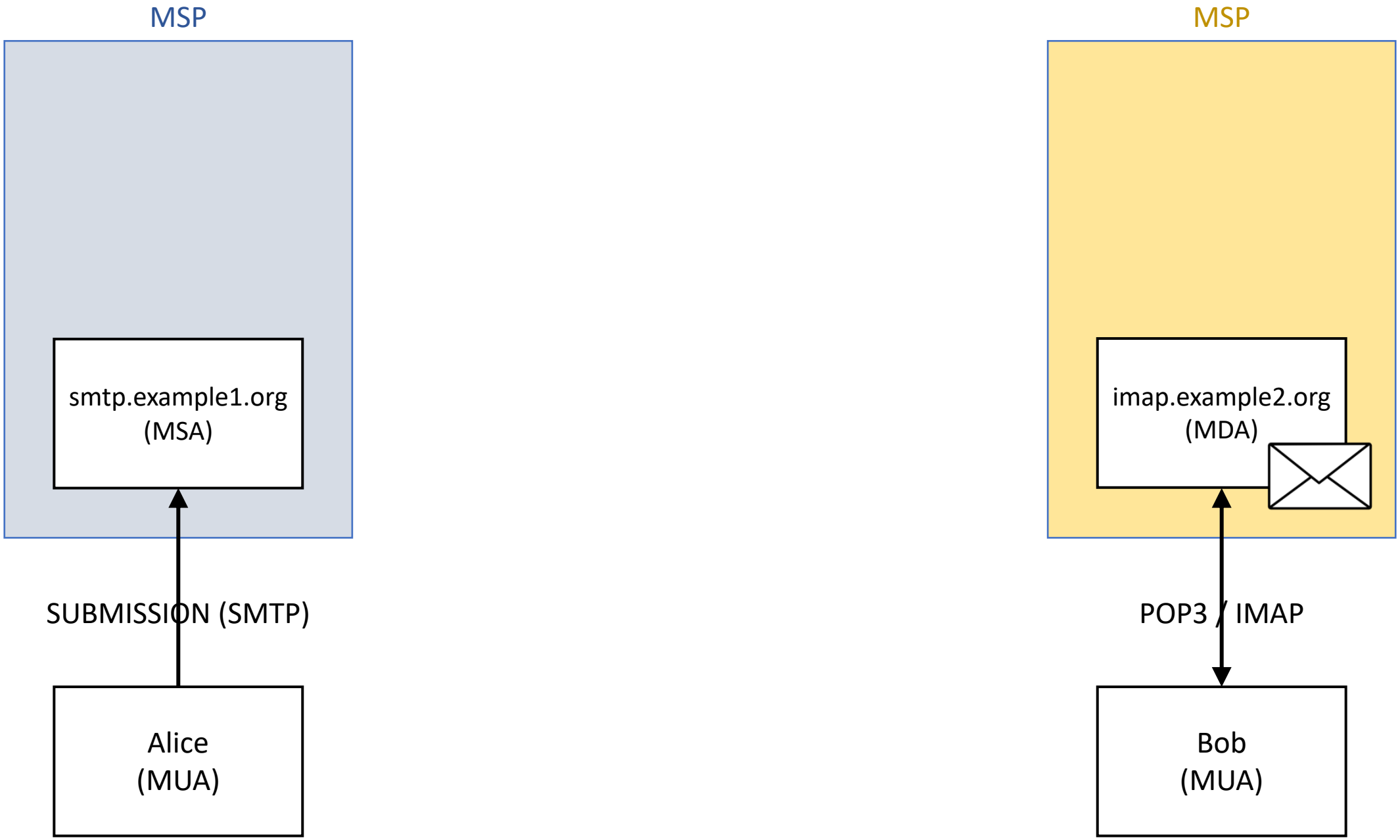
MSP

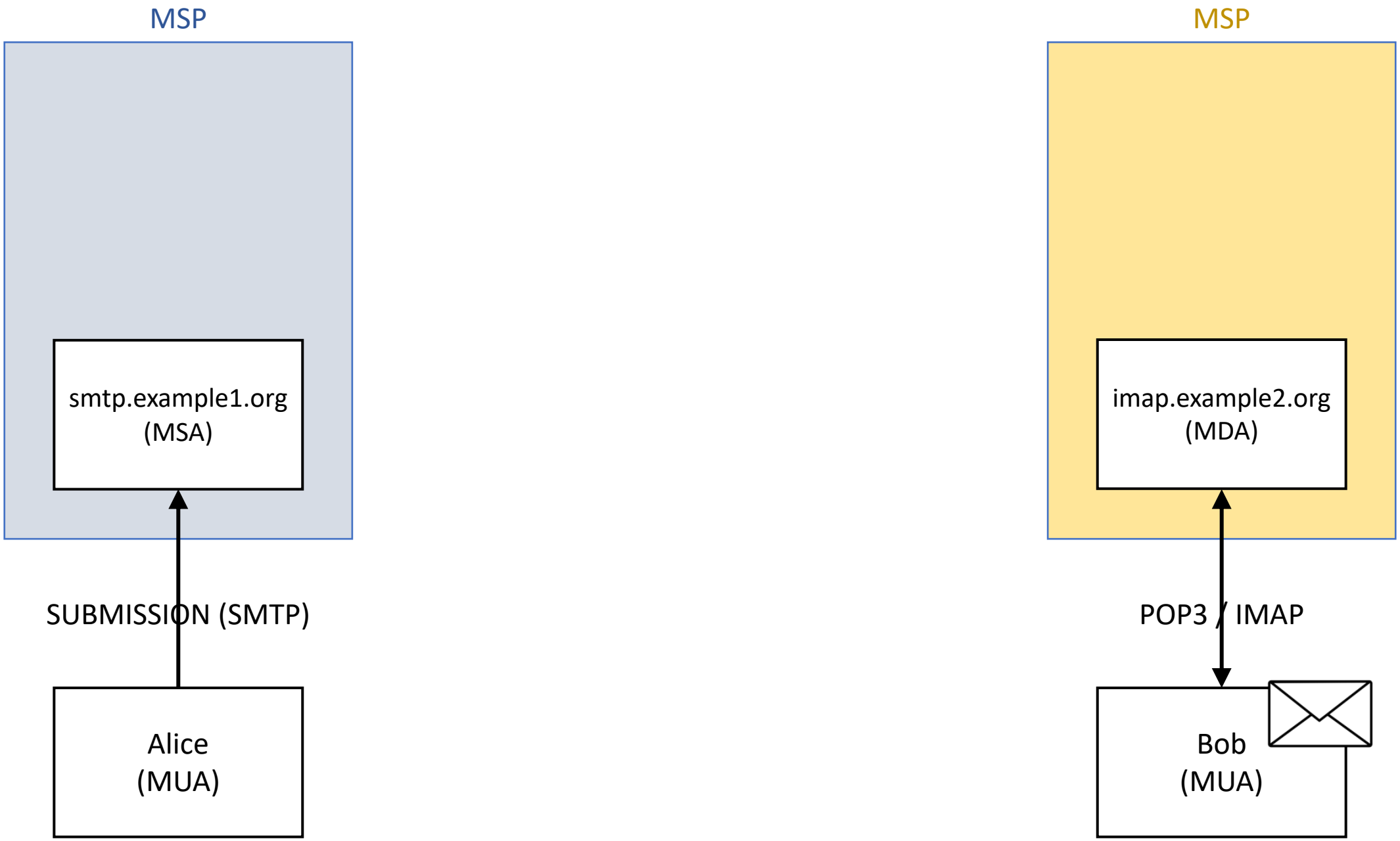


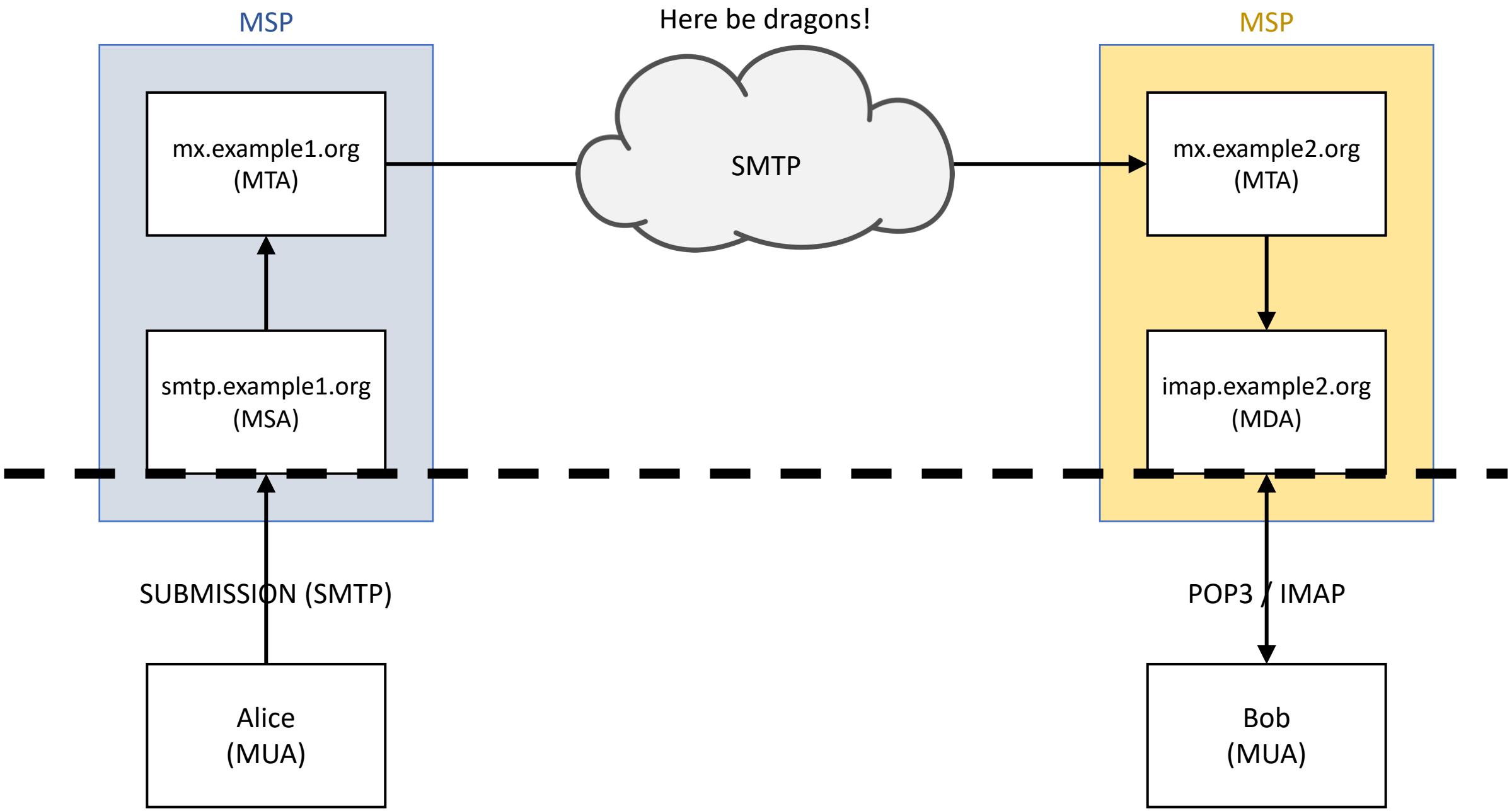
Bob
(MUA)

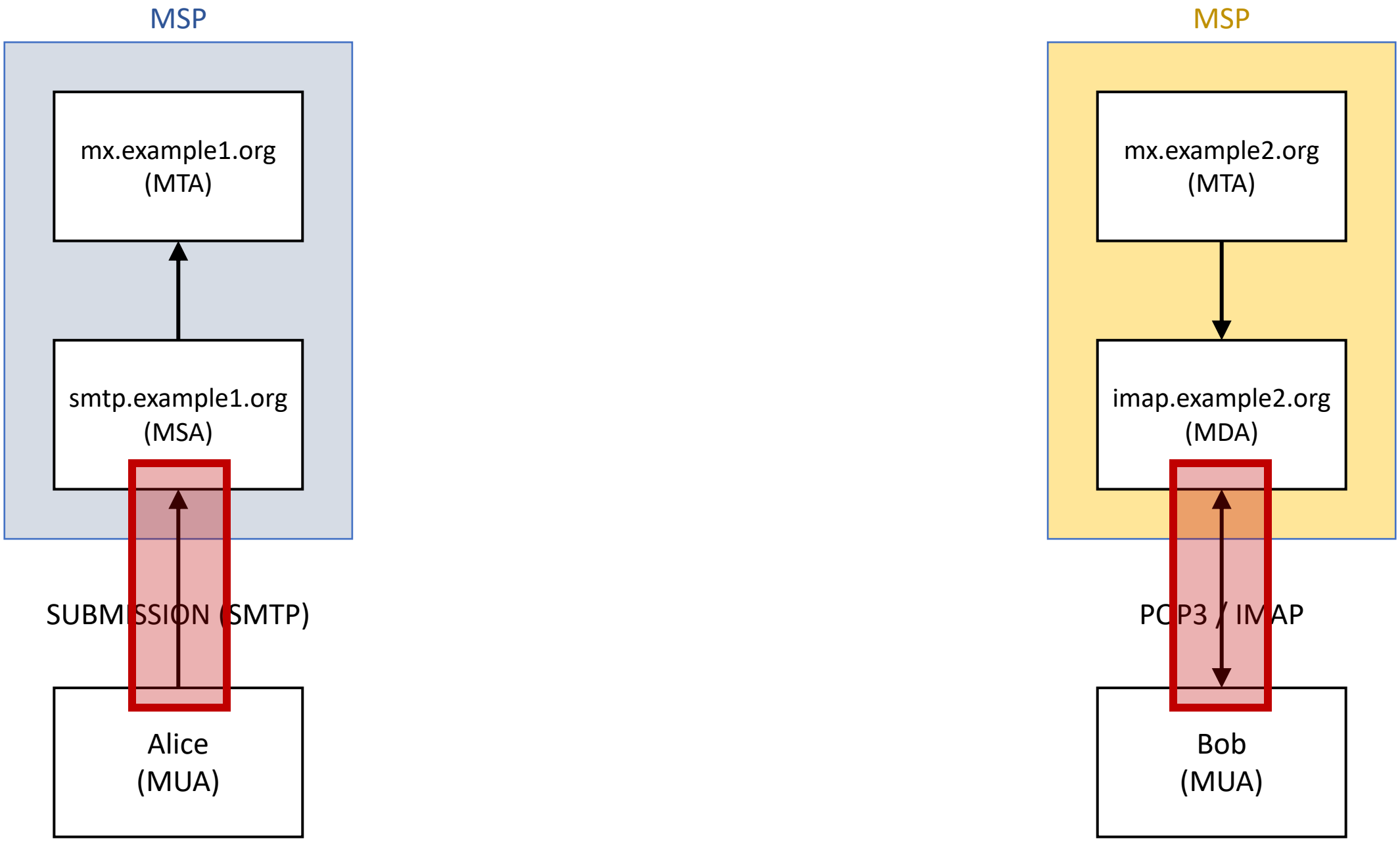

MSP
MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
Bob
(MUA)
Bestehende E-Mail-Adresse einrichten
Bestehende E-Mail-Adresse einrichten
Richten Sie Ihre derzeitige E-Mail-Adresse ein.
Ihr Name:
Alice
E-Mail-Adresse:
alice@example.org
Passwort:
Passwort speichern
Ihr Benutzername:
IHREDOMÄNE\ihrbenutzername
POSTEINGANGS-SERVER:
POSTAUSGANGS-SERVER:
Protokoll:
IMAP
SMTP
Server:
imap.example.org
smtp.example.org
Port:
143
587
SSL:
STARTTLS
STARTTLS
Authentifizierung:
Automatisch erkennen
Benutzername:
alice@example.org
Automatisch erkennen
Keine Verbindungssicherheit
STARTTLS
SSL/TLS
Abbrechen
Erneut testen
Fertig


MSP
MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
Bob
(MUA)


MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)


MSP
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)


MSP
Here be dragons!
MSP
mx.example1.org
(MTA)
SMTP
mx.example2.org
(MTA)
smtp.example1.org
(MSA)
imap.example2.org
(MDA)
SUBMISSION (SMTP)
POP3 / IMAP
Alice
(MUA)
Bob
(MUA)


MSP
mx.example1.org
(MTA)
smtp.example1.org
(MSA)
SUBMISSION (SMTP)
Alice
(MUA)
MSP
mx.example2.org
(MTA)
imap.example2.org
(MDA)
POP3 / IMAP
Bob
(MUA)

Email Protocols & STARTTLS

Why STARTTLS?

- SMTP, POP3, and IMAP were around **before SSL/TLS**

  ➔ Plaintext only

Protocol	Plaintext Port
SMTP (MTA-MTA)	25
Submission (MUA-MSA)	587
POP3	110
IMAP	143

Why STARTTLS?

- SMTP, POP3, and IMAP were around **before SSL/TLS**

  ➔ Plaintext only

Protocol	Plaintext Port	Implicit TLS Port
SMTP (MTA-MTA)	25	465
Submission (MUA-MSA)	587	465
POP3	110	995
IMAP	143	993

Why STARTTLS?

- SMTP, POP3, and IMAP were around **before SSL/TLS**
  - ➔ Plaintext only
  - STARTTLS was added in 1998/1999

Protocol	Plaintext/STARTTLS Port	Implicit TLS Port
SMTP (MTA-MTA)	25	~~465~~
Submission (MUA-MSA)	587	?
POP3	110	995
IMAP	143	993

Why STARTTLS?

- SMTP, POP3, and IMAP were around **before SSL/TLS**
  - ➔ Plaintext only
  - STARTTLS was added in 1998/1999


Opportunistic TLS

From Wikipedia, the free encyclopedia
(Redirected from Starttls)

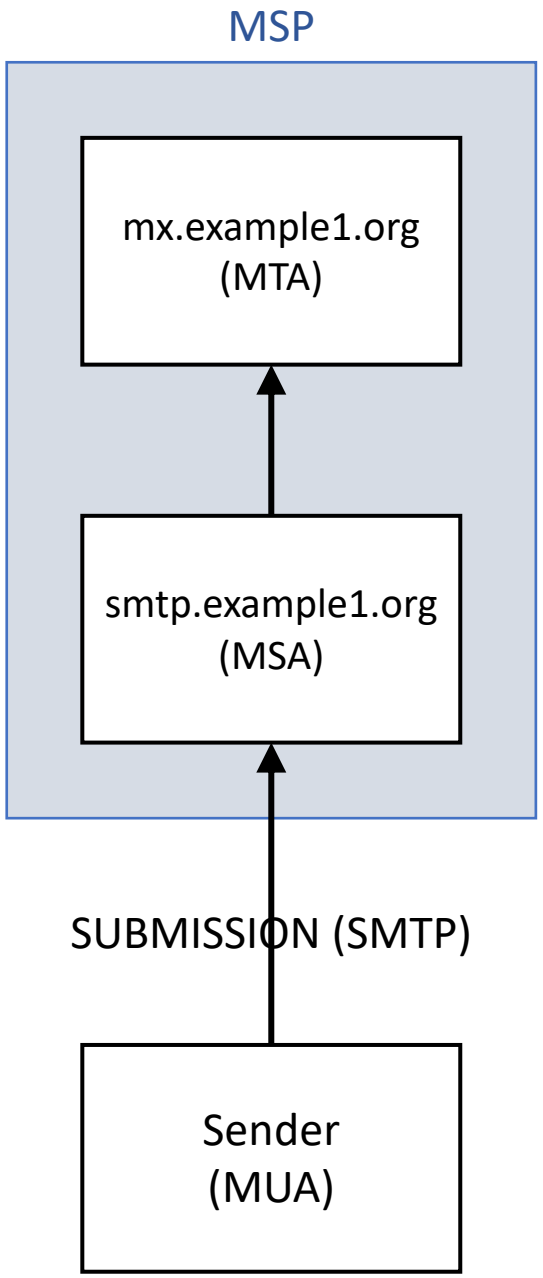
"STARTTLS" redirects here.

Protocol	Plaintext/STARTTLS Port	Implicit TLS Port
SMTP (MTA-MTA)	25	~~465~~
Submission (MUA-MSA)	587	?
POP3	110	995
IMAP	143	993

Why STARTTLS?

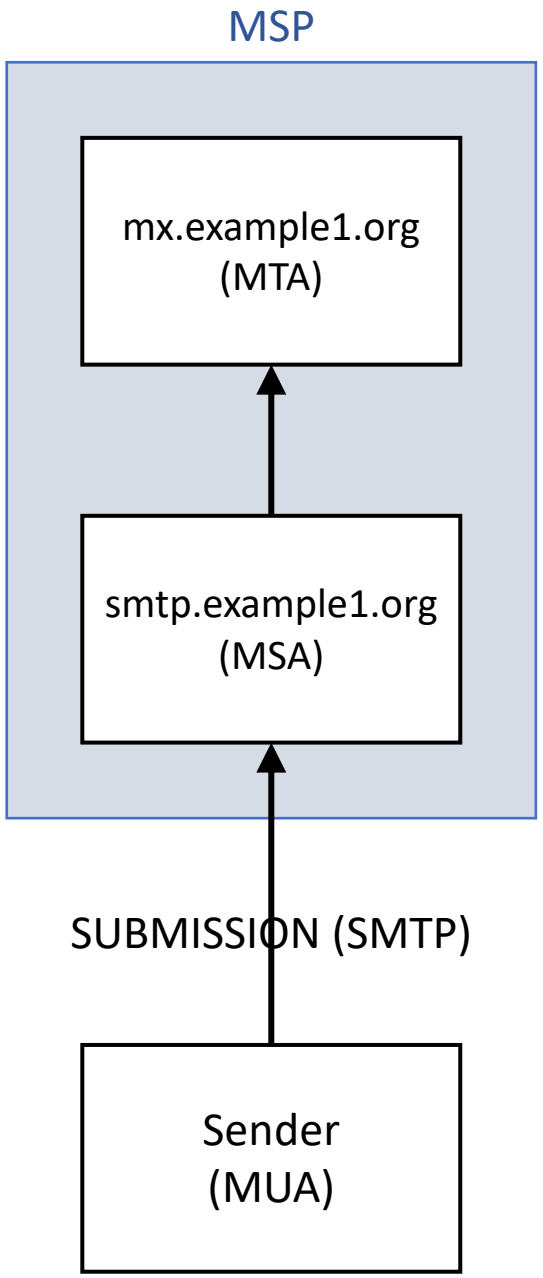
- SMTP, POP3, and IMAP were around **before SSL/TLS**
  - ➔ Plaintext only
  - STARTTLS was added in 1998/1999

Protocol	Plaintext/STARTTLS Port	Implicit TLS Port
SMTP (MTA-MTA)	25	?
Submission (MUA-MSA)	587	465
POP3	110	995
IMAP	143	993

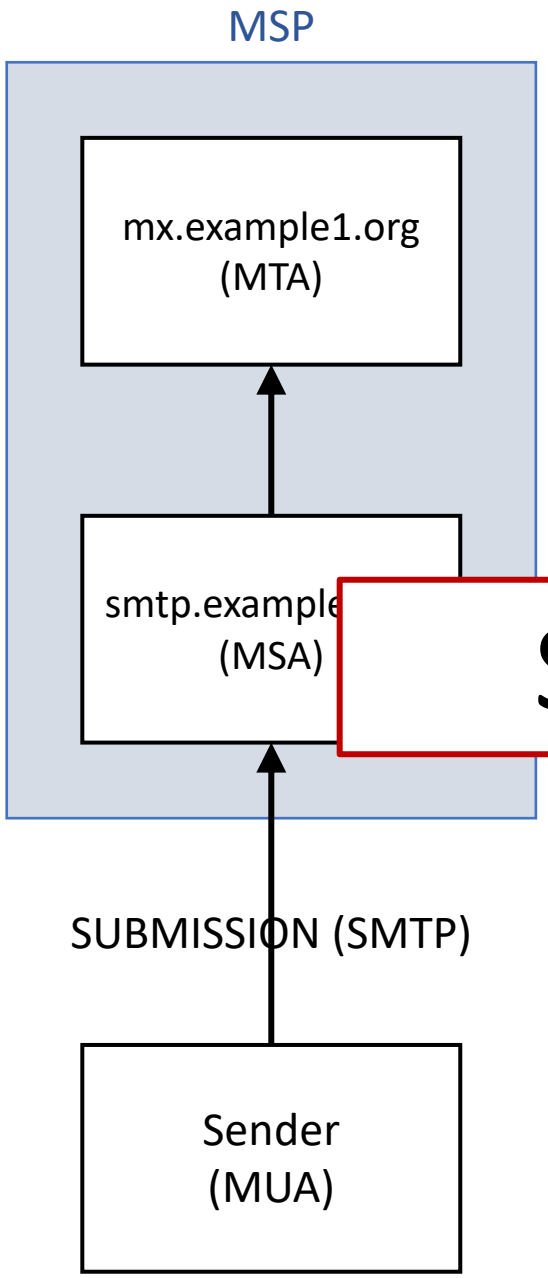



```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
```

Plaintext

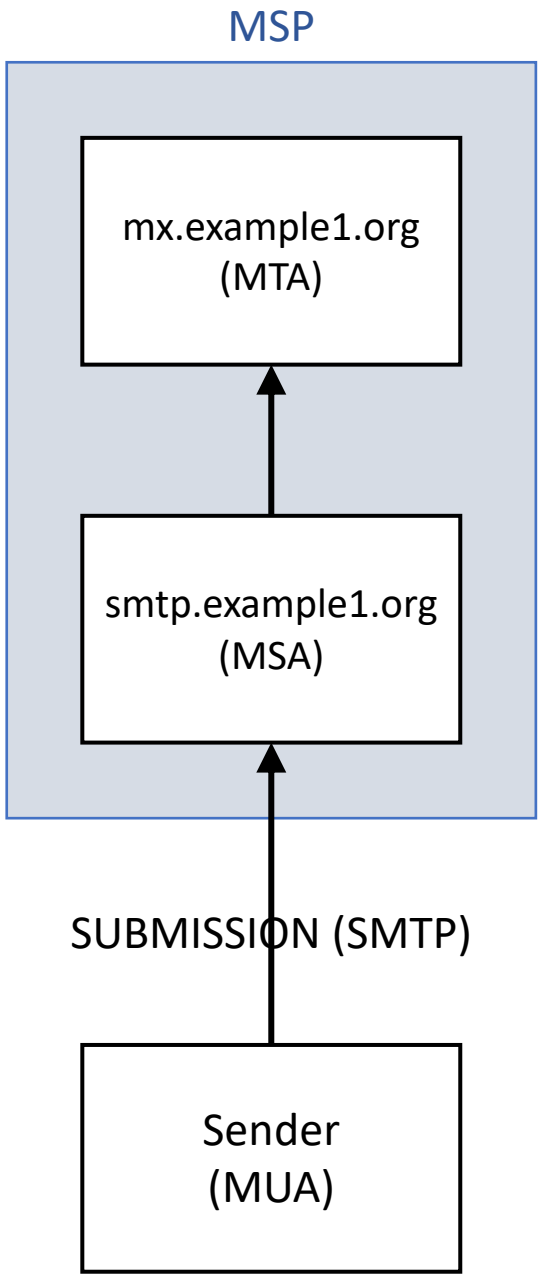



```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```



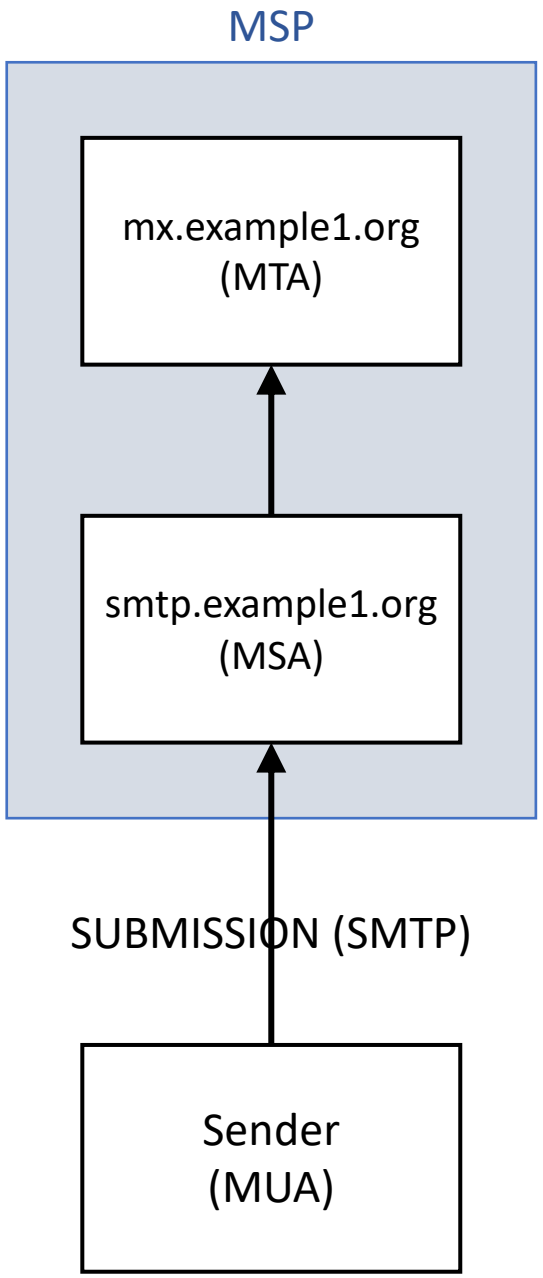

```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```

Seems easy enough!



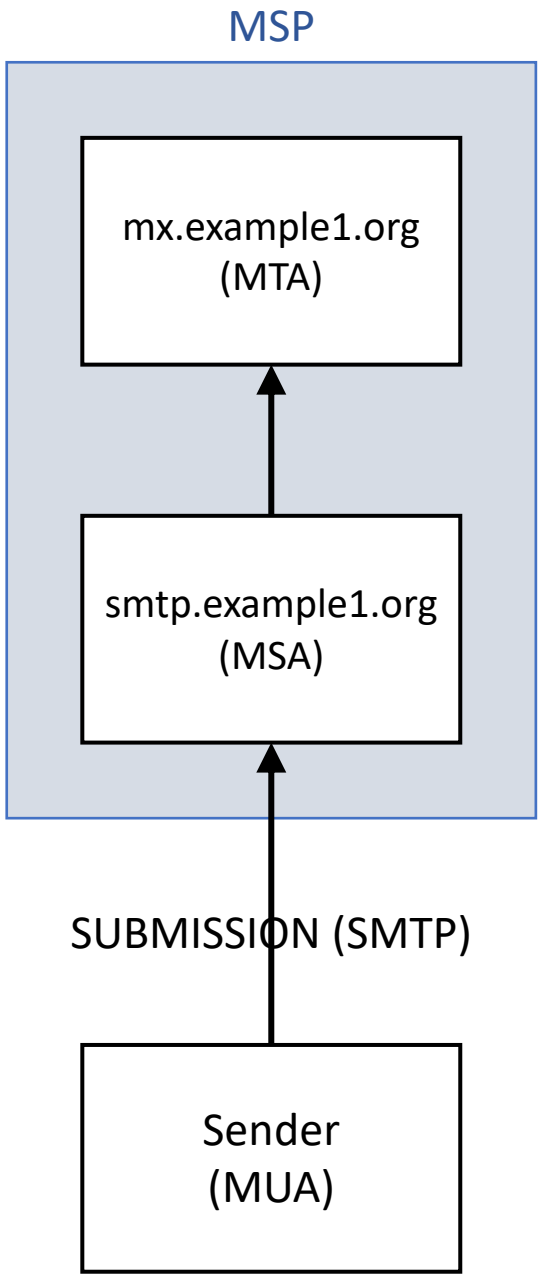

```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
```

```
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```

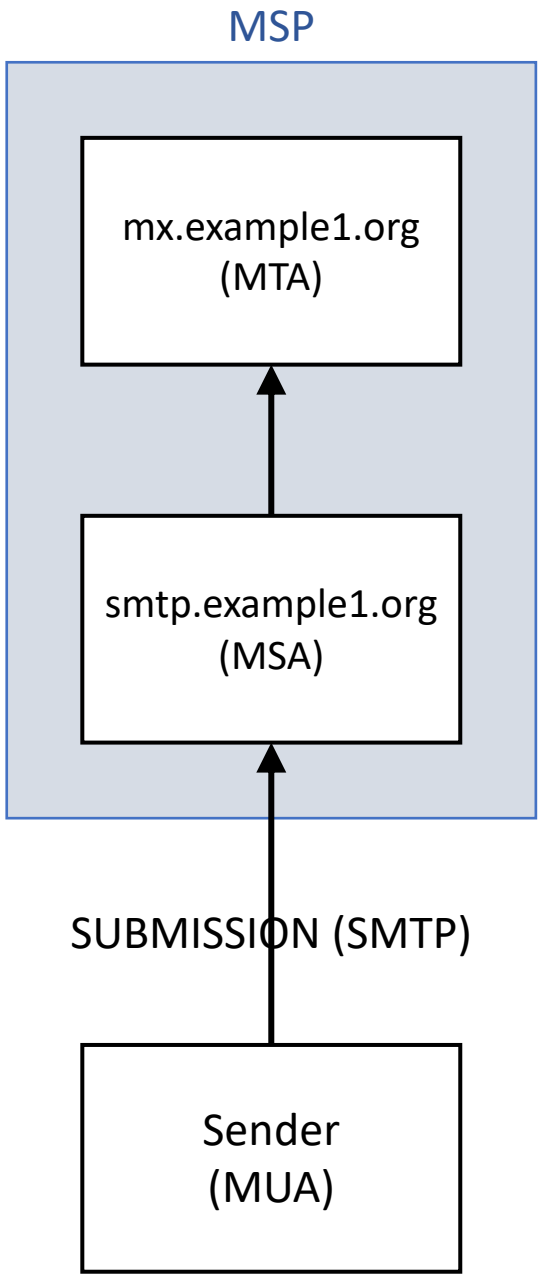



```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
```

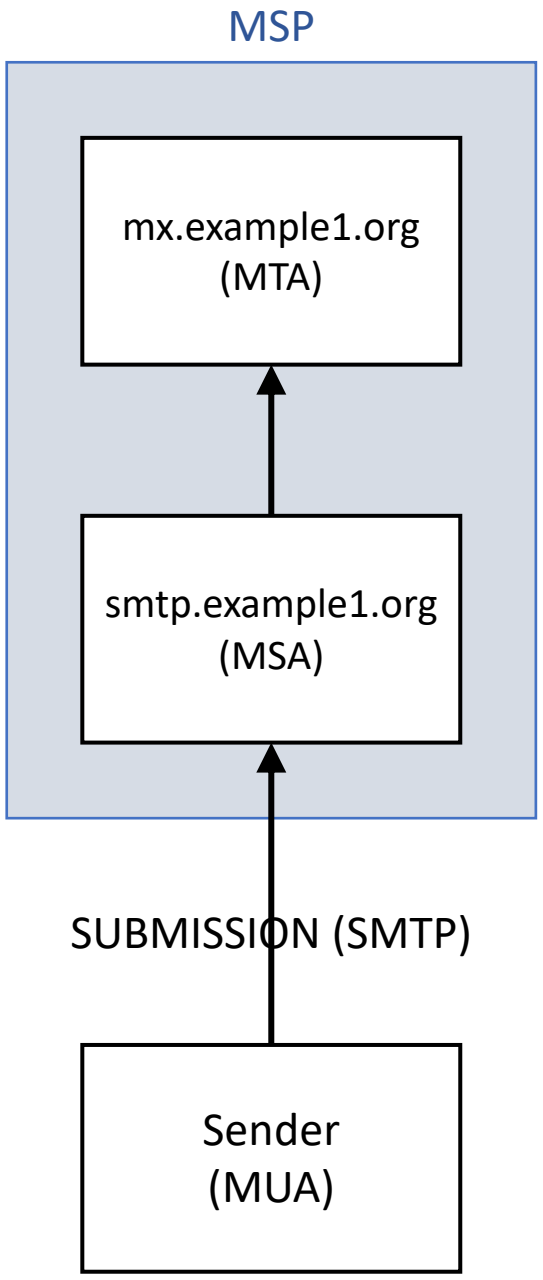
```
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```



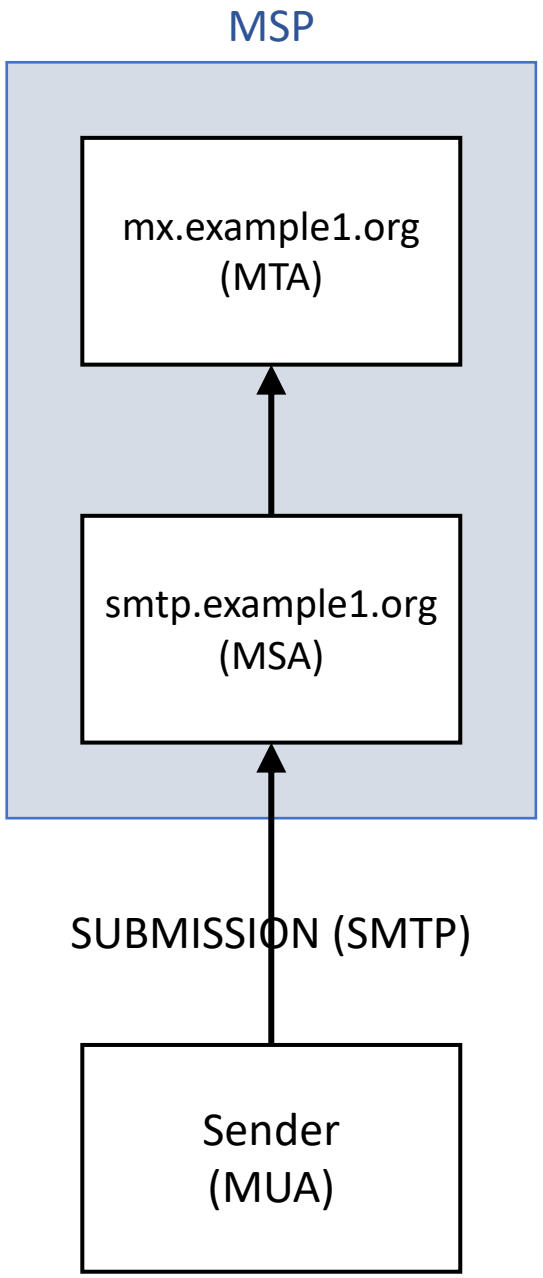

```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```



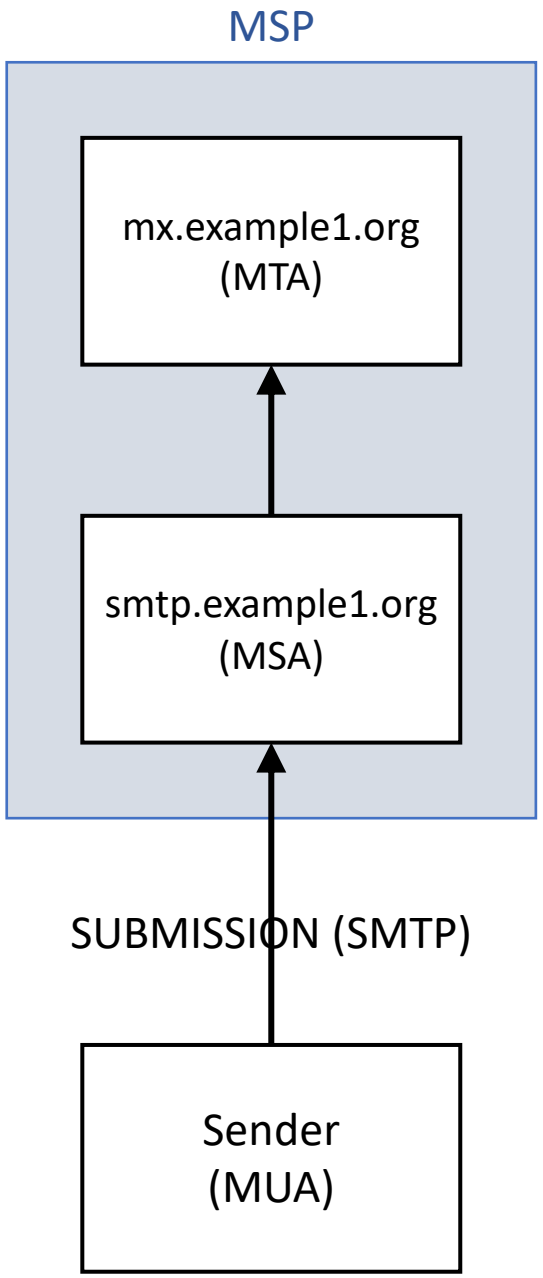

```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 454 TLS not available
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```



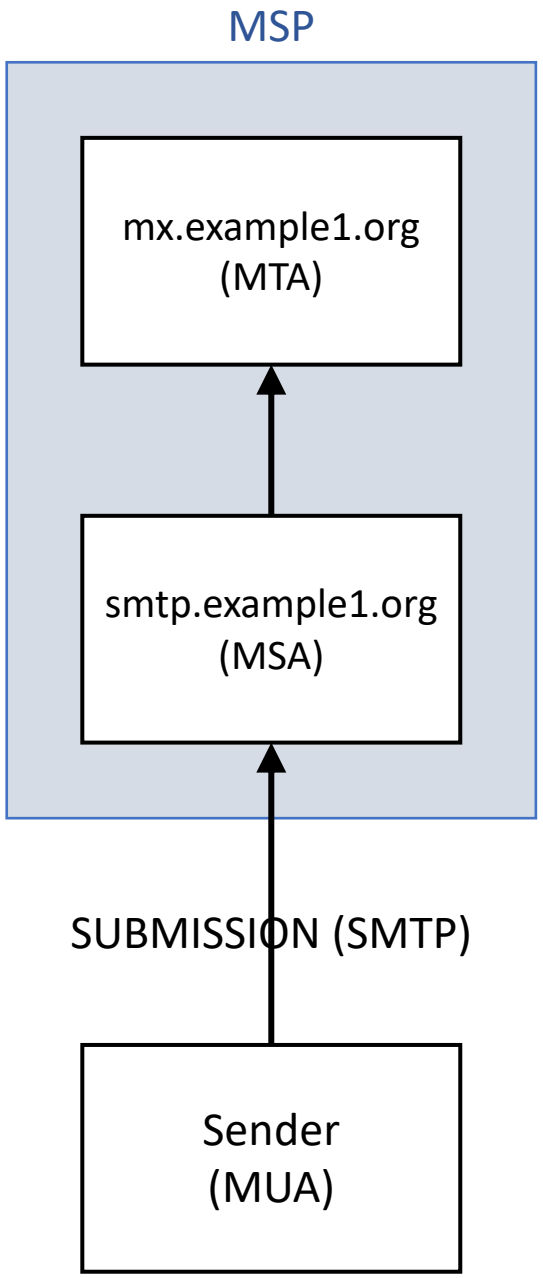

```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```




```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250-INSECURE
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 ...
C: MAIL FROM:<alice@example1.org>
S: 250 ...
C: RCPT TO:<bob@example2.org>
S: 250 ...
C: DATA
S: 354 ...
C: |Email data|
```

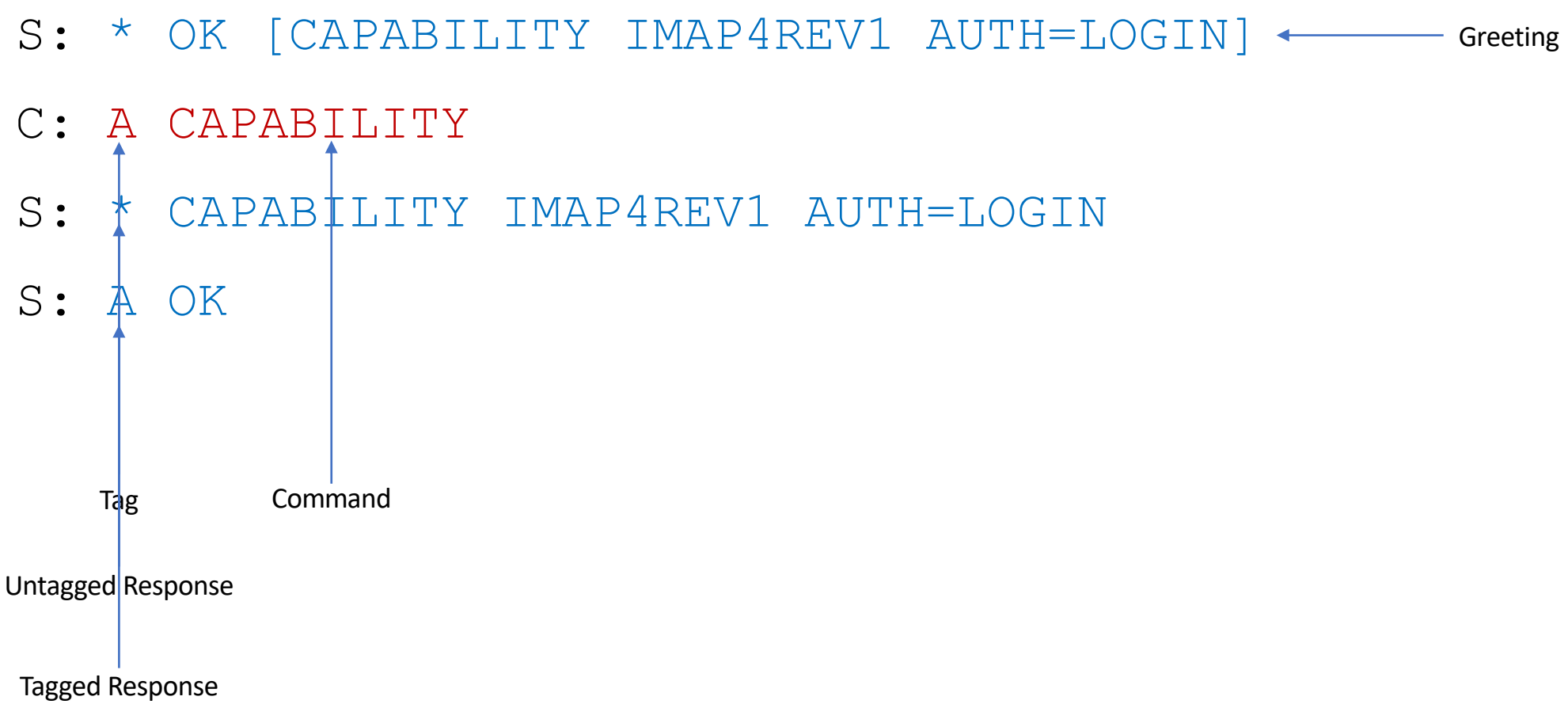



```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 OK
C: MAIL FROM:<alice@example1.org>
S: 250 OK
C: RCPT TO:<bob@example2.org>
S: 250 OK
C: DATA
S: 354 OK
C: |Email data|
```




```
S: 220 smtp.example.org ...
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 STARTTLS
C: STARTTLS
S: 220 OK
.. 235 INSECURE
// ---------- TLS Handshake ----------
C: EHLO [127.0.0.1]
S: 250-smtp.example.org ...
.. 250 AUTH PLAIN
C: AUTH PLAIN 0x00Alice0x00Password
S: 235 ...
C: MAIL FROM:<alice@example1.org>
S: 250 ...
C: RCPT TO:<bob@example2.org>
S: 250 ...
C: DATA
S: 354 ...
C: |Email data|
```

IMAP


S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]
Greeting
C: A CAPABILITY
S: * CAPABILITY IMAP4REV1 AUTH=LOGIN
S: A OK
Tag
Command
Untagged Response
Tagged Response

STARTTLS

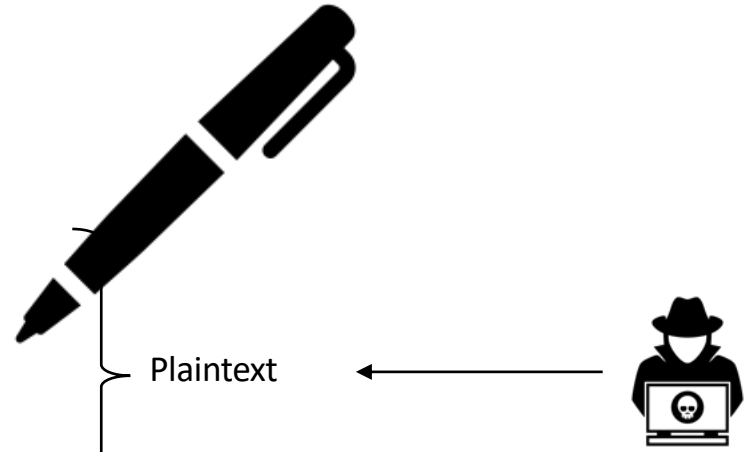
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```

Plaintext

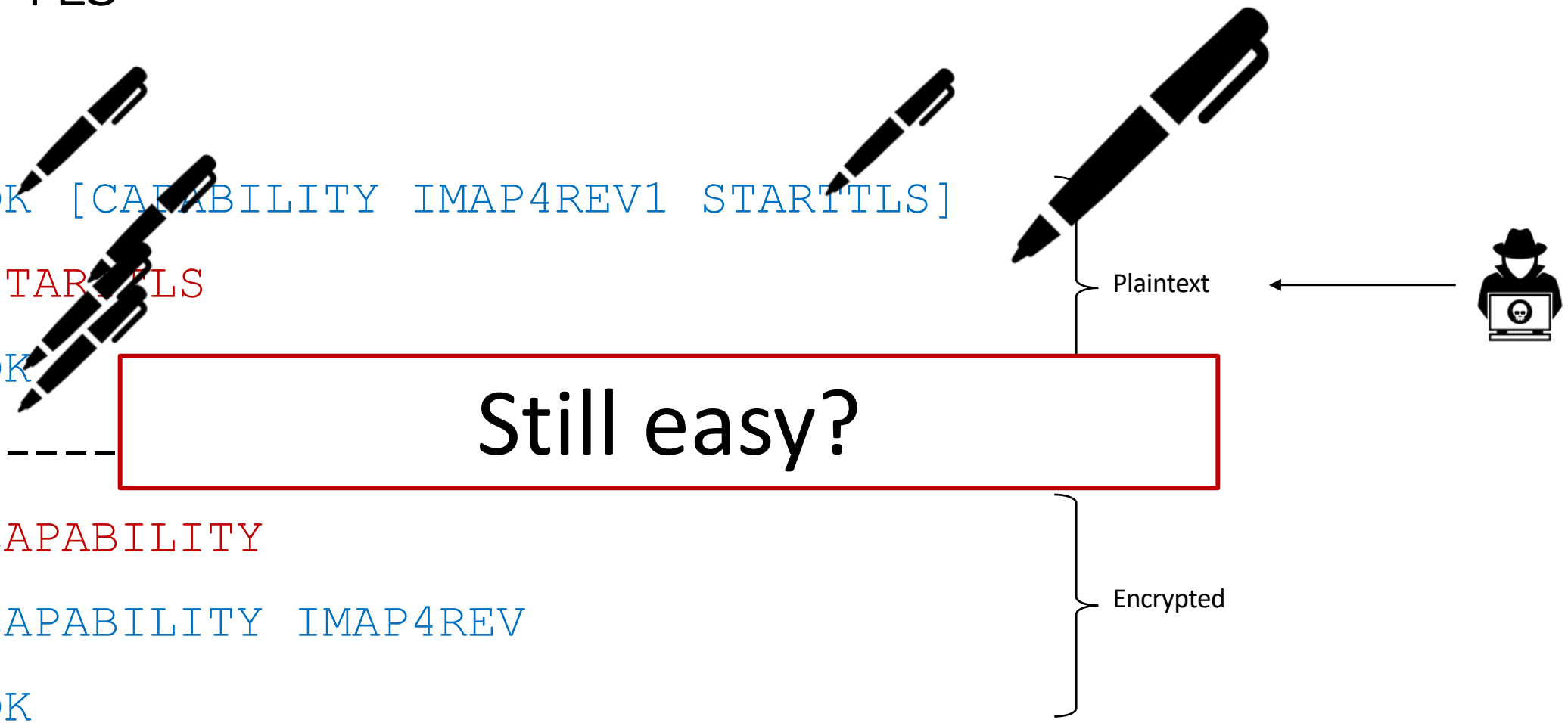
Encrypted

STARTTLS

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
```



STARTTLS


S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// -------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
Plaintext
Encrypted
Still easy?

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

Why TLS is better without STARTTLS: A Security Analysis of STARTTLS in the Email Context

Damian Poddebniak and Fabian Ising, *Münster University of Applied Sciences;*
Hanno Böck, *Independent Researcher;* Sebastian Schinzel, *Münster University of Applied Sciences*

https://www.usenix.org/conference/usenixsecurity21/presentation/poddebniak

Research Questions

Are modern clients opportunistic?

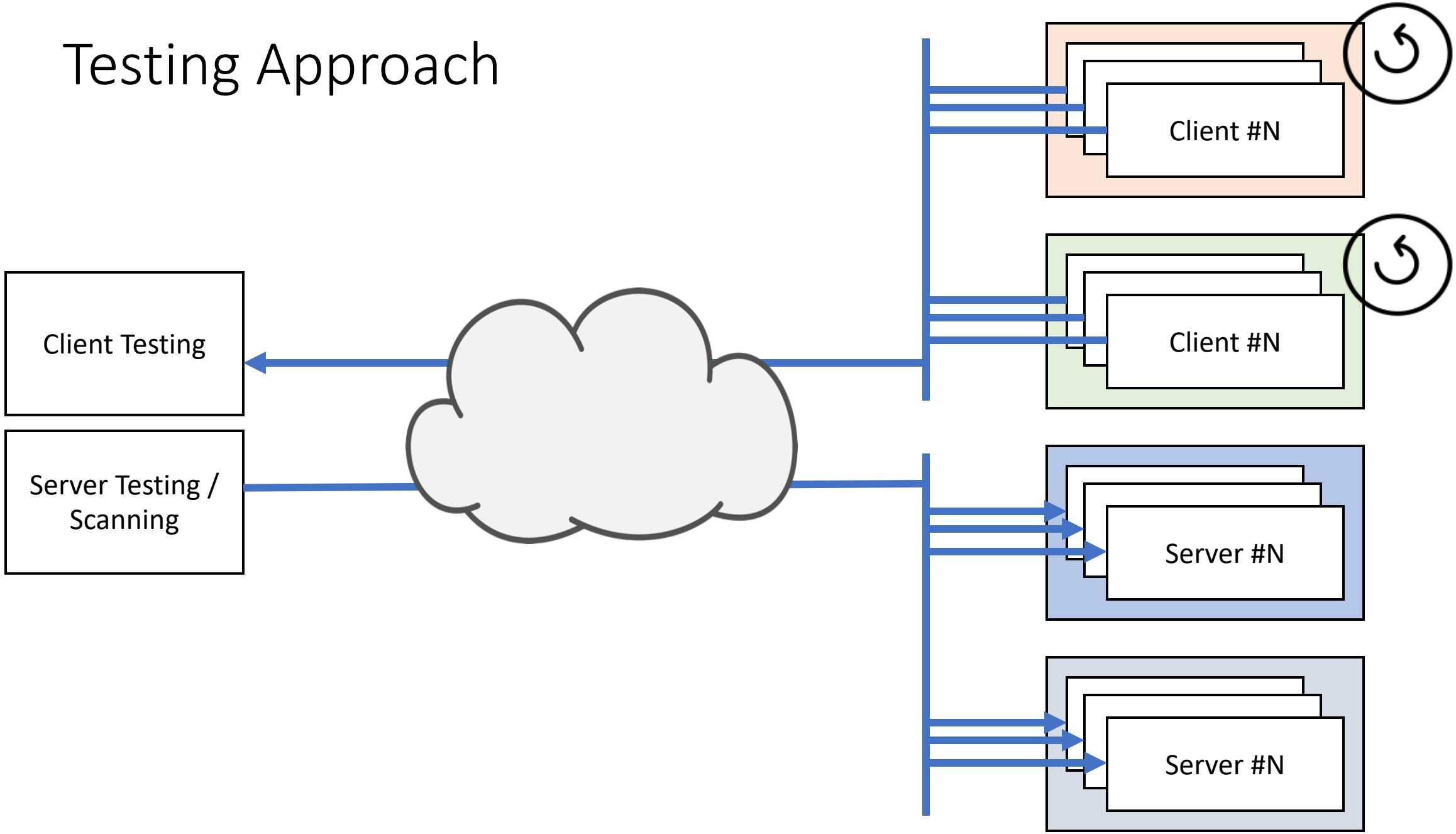
What data is sent in plaintext?

What is retained from the plaintext phase?

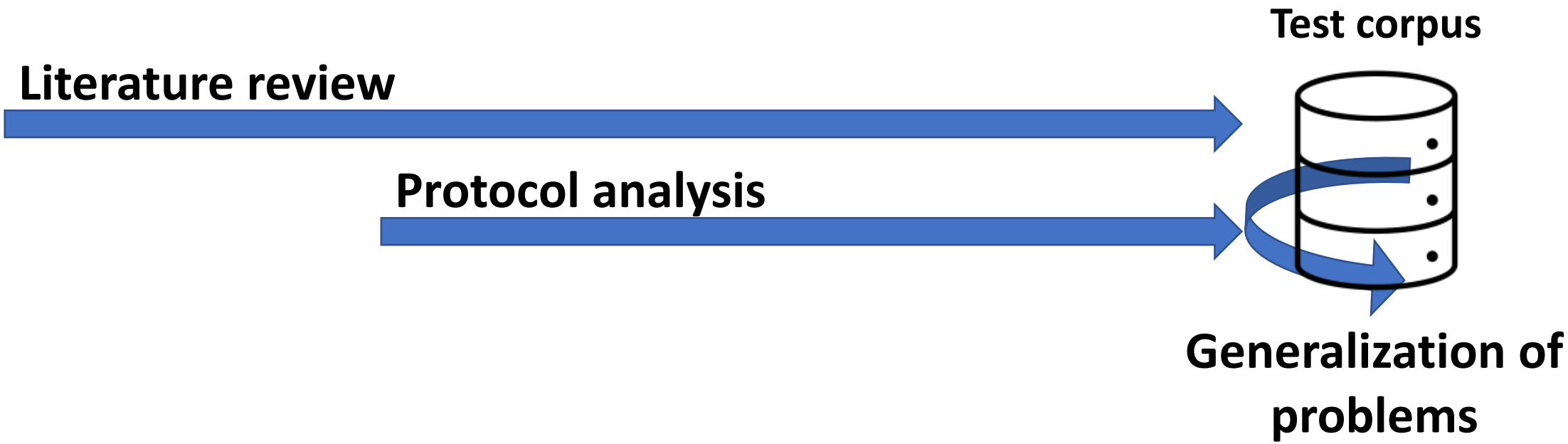
What happens in error cases?

Methodology

Testing Approach

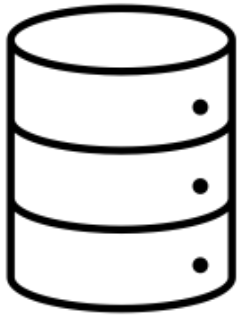


How to create a STARTTLS test corpus?



Attack Classes

Test corpus



- Negotiation
- Session Fixation
- Tampering
- UI Spoofing
- Buffering

Attacks

Negotiation

STARTTLS / Attacks

NEGOTIATION / STRIPPING #1

S: * OK [CAPABILITY IMAP4REV1 ~~STARTTLS~~]

~~C: A STARTTLS~~

~~S: A OK~~

~~// TLS Handshake~~

C: B CAPABILITY

S: * CAPABILITY IMAP4REV

.. B OK

C: C LOGIN alice password

STARTTLS / Attacks

NEGOTIATION / STRIPPING #1

```
S: * OK [CAPABILITY IMAP4REV]
```

```
C: C LOGIN alice password
```

STARTTLS / Attacks

NEGOTIATION / STRIPPING #2

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice password
```

STARTTLS / Attacks

NEGOTIATION / STRIPPING #2

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
// TLS Handshake
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice password
```

STARTTLS / Attacks

NEGOTIATION / STRIPPING #2

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A NO
```

```
C: C LOGIN alice password
```

STARTTLS / Attacks

NEGOTIATION / PREAUTH

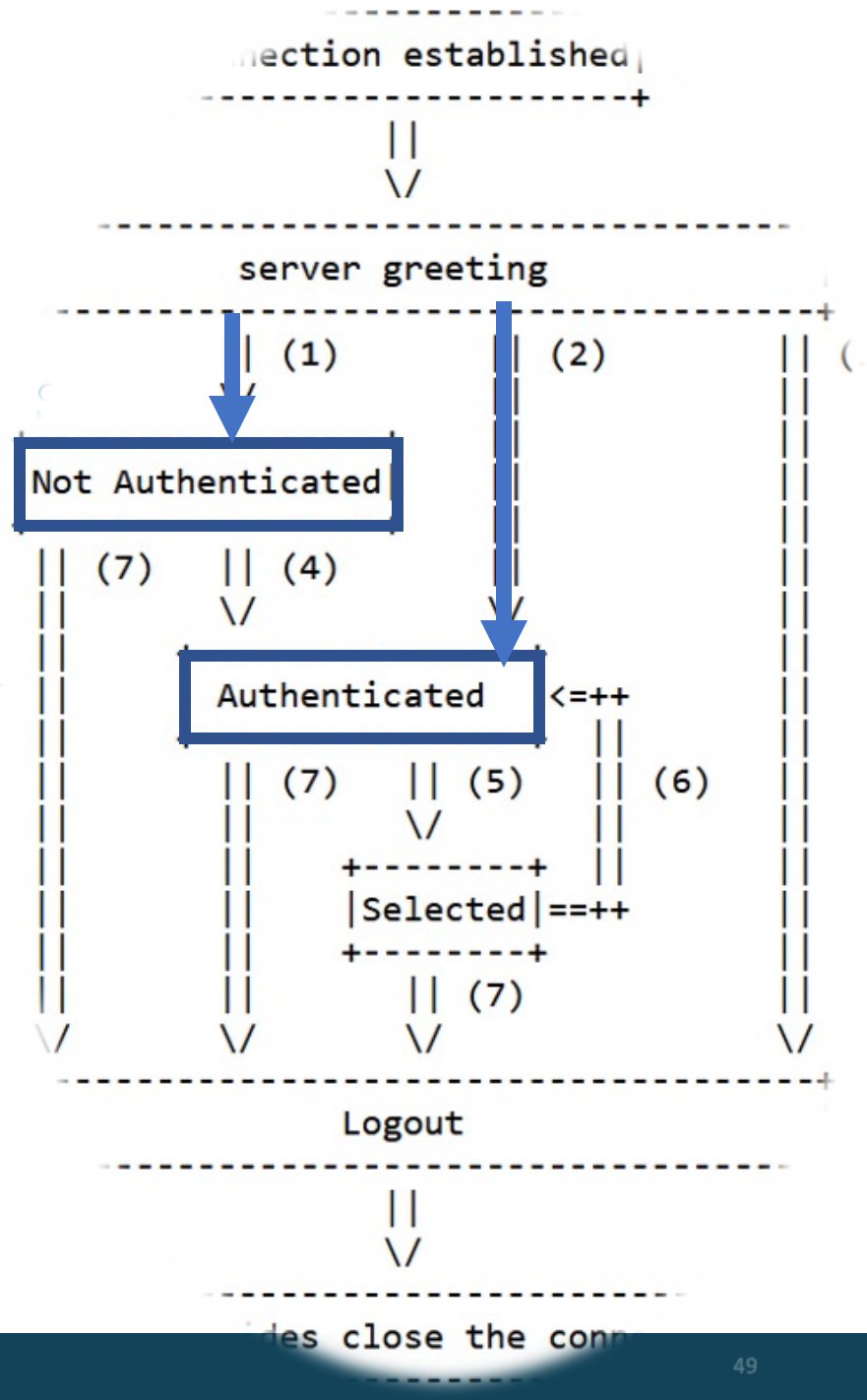
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice password
```

STARTTLS / Attacks

NEGOTIATION / PREAUTH

```
S: * ~~OK~~ PREAUTH [CAPABILITY IMAP4REV1
C: A STARTTLS
S: A OK
// ----------- TLS Handshake --------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice password
```

Violates the IMAP specification

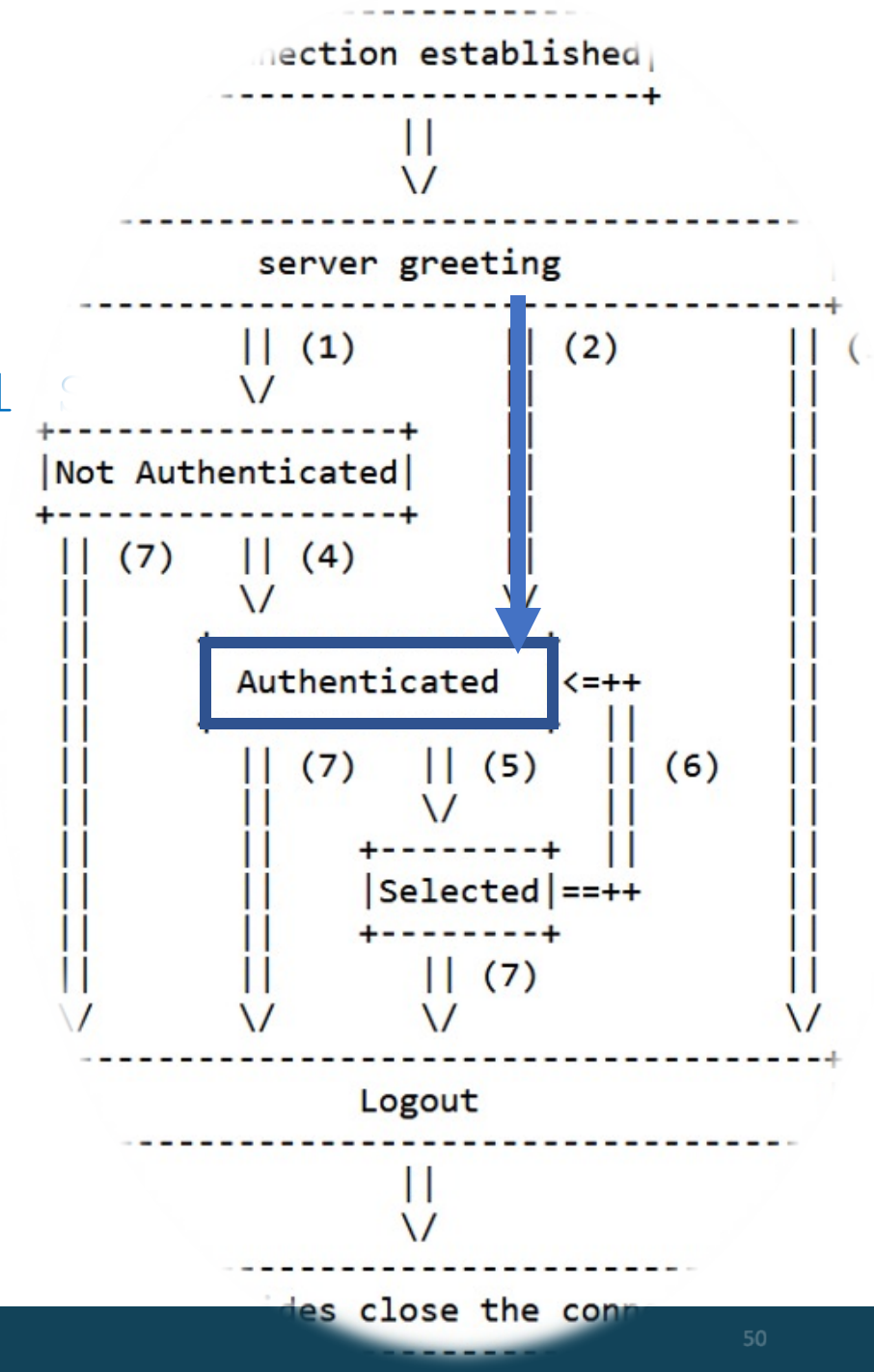


STARTTLS / Attacks

NEGOTIATION / PREAUTH

```
S: * ~~OK~~ PREAUTH [CAPABILITY IMAP4REV1
```

```
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice password
```

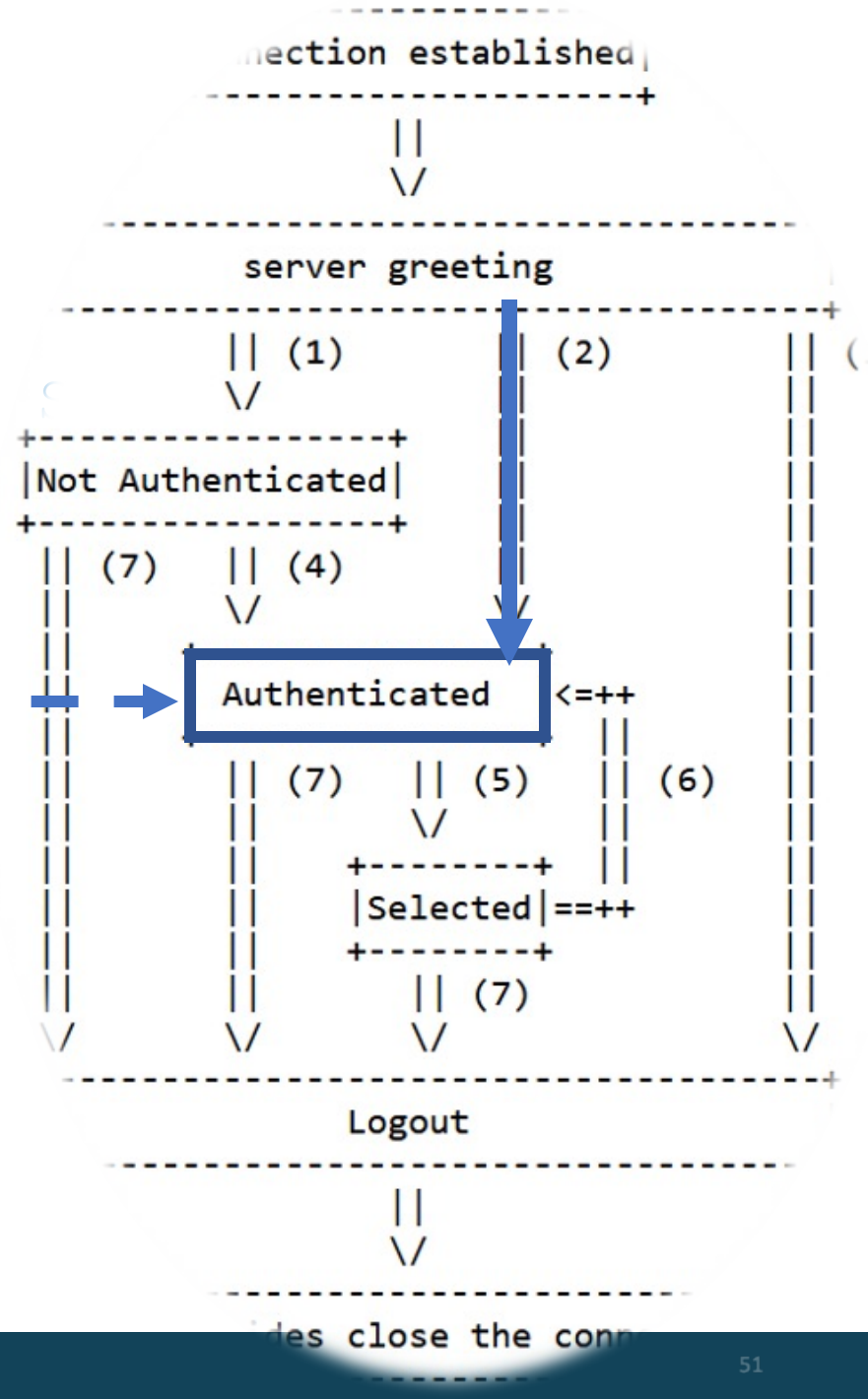


STARTTLS / Attacks

NEGOTIATION / PREAUTH

S: * ~~OK~~ *PREAUTH* [CAPABILITY IMAP4REV1

C: C LOGIN alice password

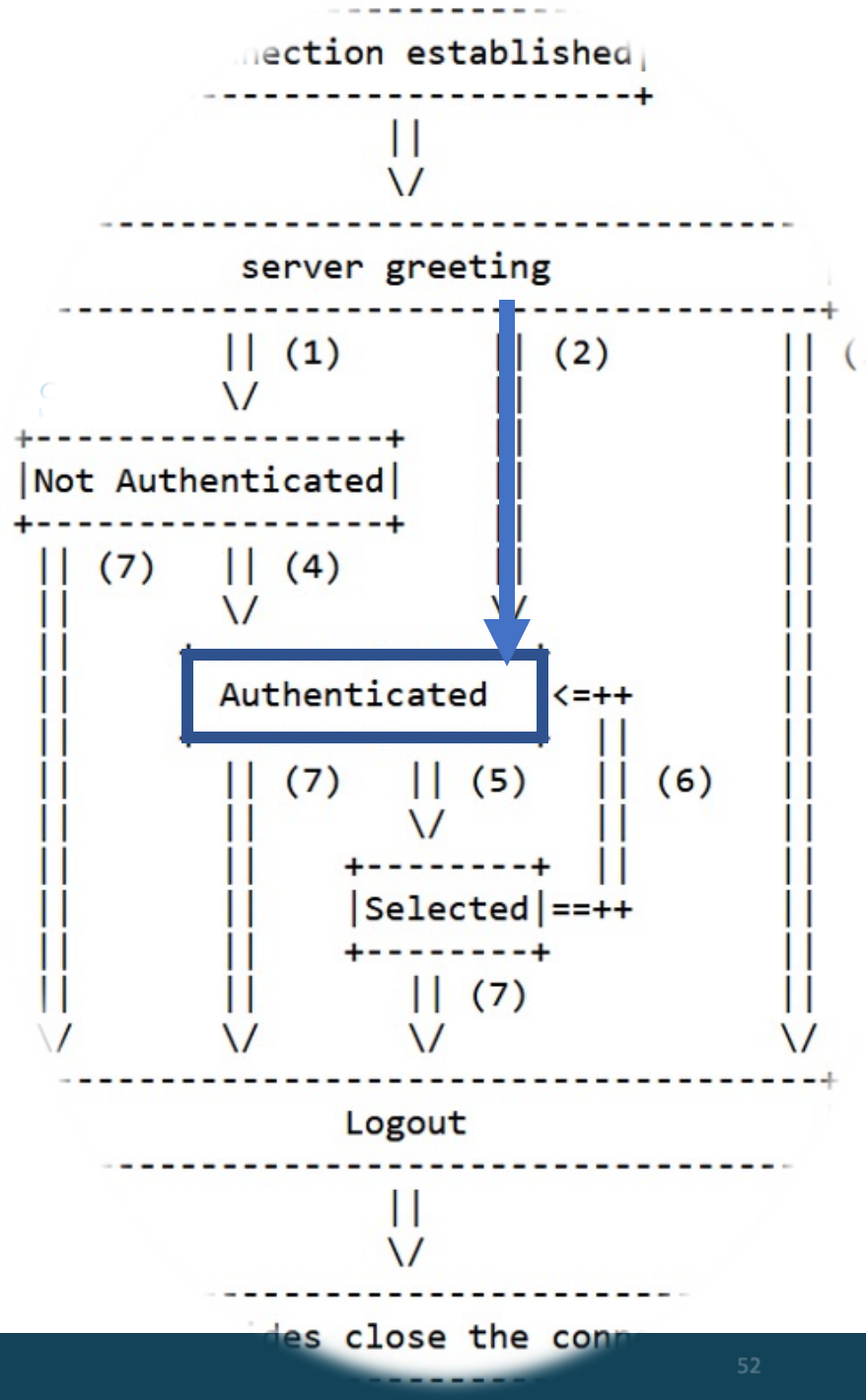


STARTTLS / Attacks

NEGOTIATION / PREAUTH

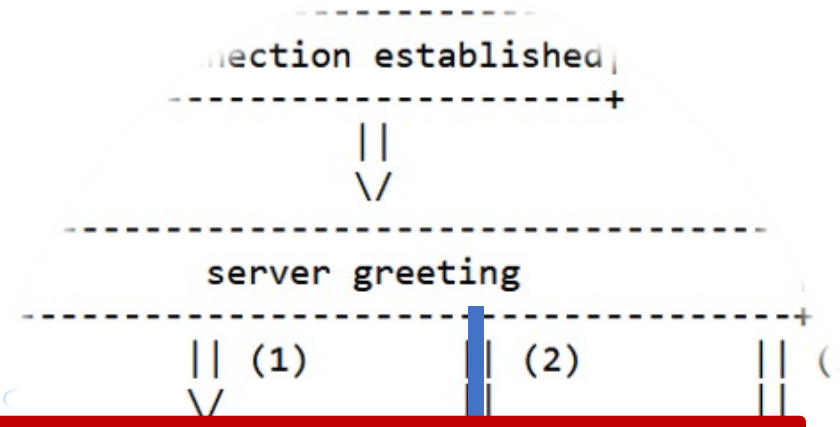
S: * ~~OK~~ *PREAUTH* [CAPABILITY IMAP4REV1

C: C SELECT INBOX



STARTTLS / Attacks

NEGOTIATION / PREAUTH




```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ---------- TLS Handshake ----------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
C: C LOGIN alice passwor
S:
```

attacker.example.org

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●N_S									
Gmail Go (8.5.6.197464524)	✓	✓	●N_S									
Samsung Email (6.1.12.1)	✓	✓	●N_S									
K-9 Mail (5.710)	✓	✓	✓									
LineageOS email (9)	✓	✓	✓									
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●N_P									
Gmail (6.0.200614)	✓	∅	✓									
Edison Mail (1.20.8)	✓	∅	TLS									
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓									
Apple macOS												
Mail (3608.80.23.2.2)	✓	✓	✓									
Linux (tested on NixOS)												
Balsa (2.5.9-1)	✓	✓	○C[1]									
Evolution (3.34.4)	✓	✓	✓									
Geary (3.34.2)	✓	∅	✓									
KMail (19.12.3)	●N_S[2]	✓	✓									
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○N_S[1]	●N_P									
Trojita (0.7.20190618)	✓	∅	✓									
Claws (3.17.4)	✓	✓	✓									
Sylpheed (3.7.0)	✓	✓	●N_S									
Alpine (2.21)	✓	✓	●N_P,N_R									
Mutt (1.13.3)	✓	✓	●N_P									
NeoMutt (20200417)	✓	✓	●N_P									
OfflineIMAP (7.3.2)	∅	∅	●N_S[3]									
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓									
Yandex.Mail	✓	∅	✓									
GMX Mail Collector	∅	●N_S	●N_S									
Mail.ru	●N_S	∅	TLS									
myMail	●N_S	∅	TLS									
Email App for Gmail	●N_S	∅	TLS									

15/28

(with varying impact)

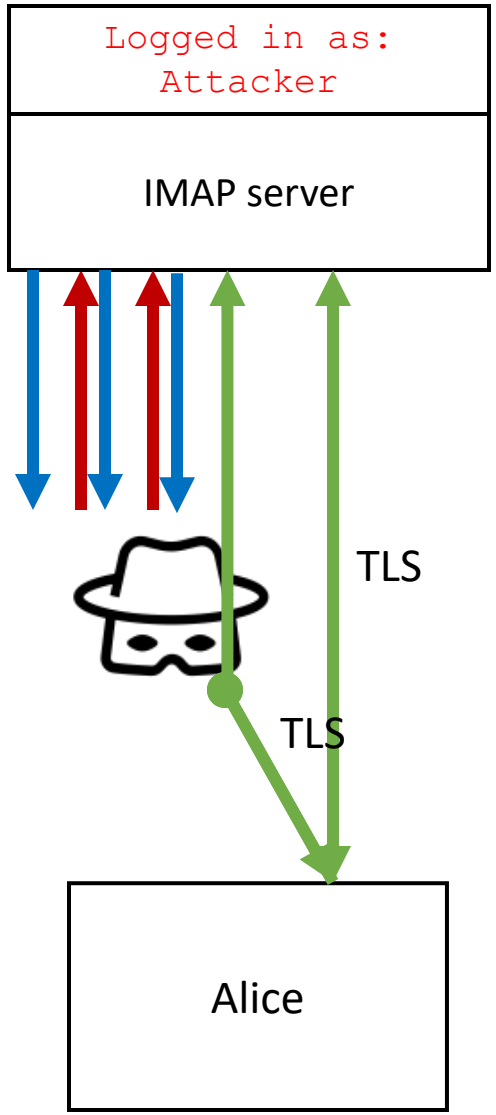
Attacks

Session Fixation

STARTTLS / Attacks

SESSION FIXATION

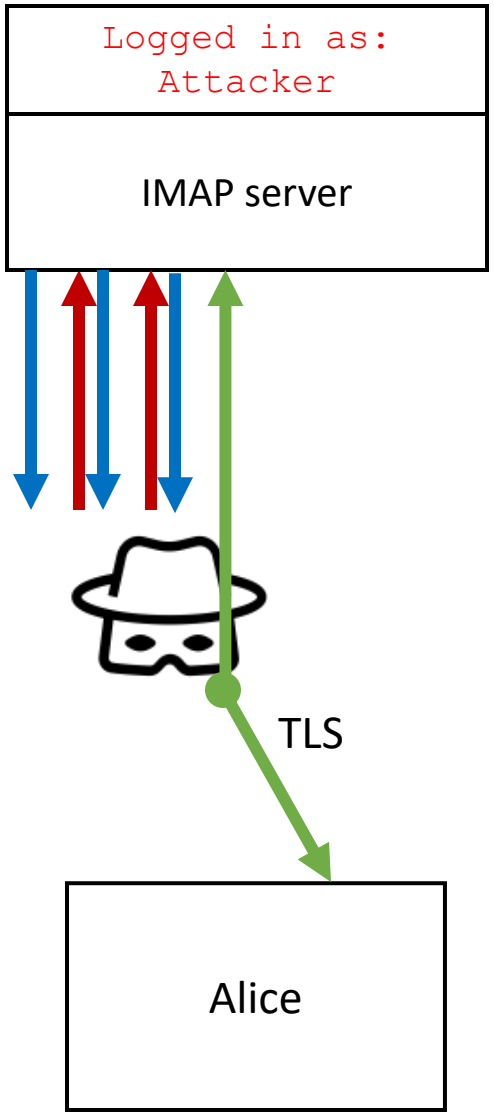
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A LOGIN attacker pa$$w0rd
S: A OK
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: ...
```



STARTTLS / Attacks

SESSION FIXATION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A LOGIN attacker pa$$w0rd
S: A OK
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: A LOGIN alice password
S: A NO already logged in as "Attacker"
```



Product	Session Fixation: SMTP	Session Fixation: POP3	Session Fixation: IMAP
Citadel (929)	◐	●	●
Courier (1.0.14)	✓	◐	✓
Exchange (2016)	✓	✓	✓
Gordano GMS[12] (20.06)	–	–	–
IceWarp (Deep Castle 2)	◐	✓	✓
[illegible]	◐	●	●
[illegible]	✓	✓	✓
[illegible]	◐	✓	✓
[illegible]	✓	✓	✓
[illegible]	◐	◐	✓
[illegible]	✓	✓	✓
[illegible]	✓	◐	✓
[illegible]	✓	∅	∅
[illegible]	◐	∅	∅
Postfix (3.5.4)	✓	∅	∅
Qmail Toaster (1.4.1)	–	∅	∅
Qmail Toaster (1.03-3.3.1)	✓	∅	∅
Sendmail (8.16.1)	–	∅	∅
spamdyke (5.0.1)	✓	∅	∅
s/qmail (4.0.7)	✓	∅	∅
Cyrus IMAP (3.2.2)	∅	◐	✓
Dovecot (2.3.10.1)	∅	◐	✓
Mercury/32 (4.80.149)	∅	◐	✓

11/23

(with varying impact)

– Unknown / Untested
✓ No vulnerability found
◐ Historic vulnerability (fixed)
◐ No working exploit
∅ Protocol not available
● New vulnerability

Attack Class

Tampering

STARTTLS / Attacks

TAMPERING / FETCH

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: ...
```

STARTTLS / Attacks

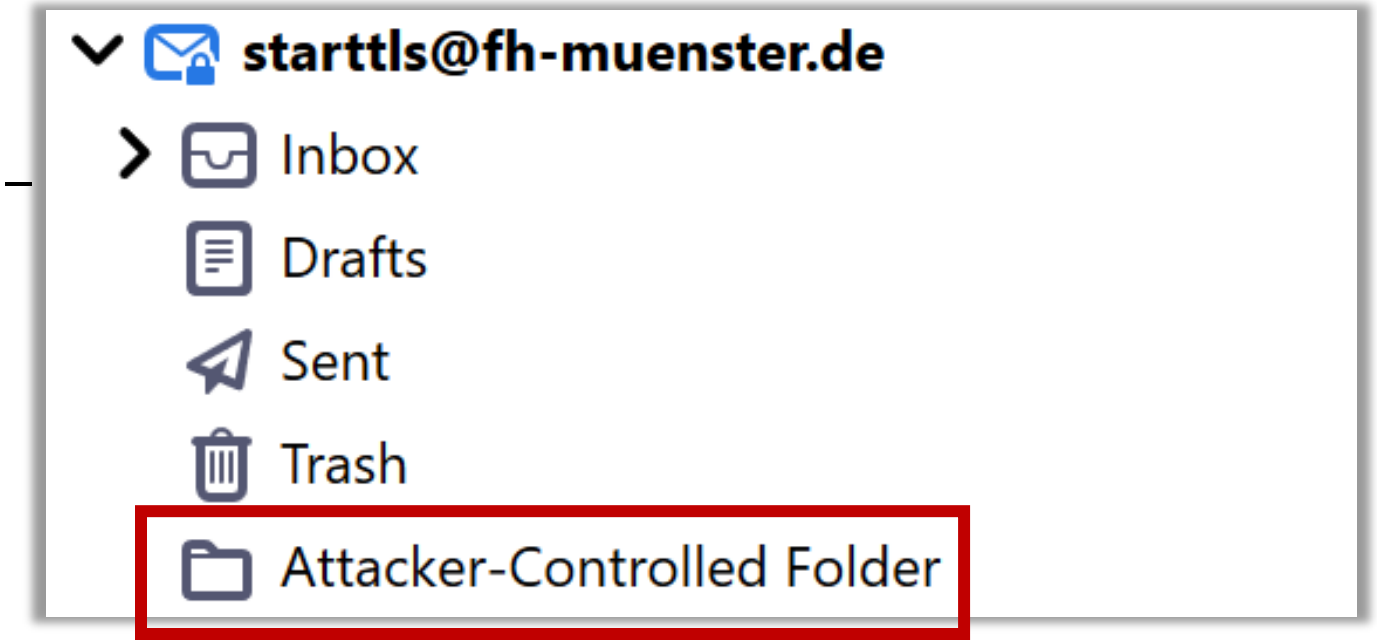
TAMPERING / FETCH

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. * 42 FETCH (BODY[] "From: Attacker\n\nHello, ...")
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: ...
```

STARTTLS / Attacks

TAMPERING / LIST

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. * LIST () “Attacker-Controlled Folder”
C: A STARTTLS
S: A OK
// ------------
C: ...
```



Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●N_S				✓	✓	✓			
Gmail Go (8.5.6.197464524)	✓	✓	●N_S				✓	✓	✓			
Samsung Email (6.1.12.1)	✓	✓	●N_S				✓	✓	✓			
K-9 Mail (5.710)	✓	✓	✓				✓	✓	✓			
LineageOS email (9)	✓	✓	✓				✓	✓	✓			
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●N_P				✓	✓	✓			
Gmail (6.0.200614)	✓	∅	✓				✓	✓	✓			
Edison Mail (1.20.8)	✓	∅	TLS				✓	✓	TLS			
Windows												
Outlook (16.0.13001.20338)								TLS	✓			
Apple macOS												
Mail (3608.80.23.2.2)								✓	✓			
Linux (tested on NixOS)												
Balsa (2.5.9-1)								✓	○$_C$			
Evolution (3.34.4)								✓	◐$_{T_M}$			
Geary (3.34.2)								∅	✓			
KMail (19.12.3)	●$_{N_S}$[2]	✓	✓				✓	✓	✓			
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]	●$_{N_P}$				✓	✓	◐$_{T_M}$			
Trojita (0.7.20190618)	✓	∅	✓				✓	∅	◐$_{T_M}$			
Claws (3.17.4)	✓	✓	✓				✓	✓	✓			
Sylpheed (3.7.0)	✓	✓	●$_{N_S}$				✓	✓	✓			
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$				✓	✓	◐$_{T_M,C}$			
Mutt (1.13.3)	✓	✓	●$_{N_P}$				✓	✓	✓			
NeoMutt (20200417)	✓	✓	●$_{N_P}$				✓	✓	✓			
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]				∅	∅	✓			
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓				✓	✓	✓			
Yandex.Mail	✓	∅	✓				✓	✓	✓			
GMX Mail Collector	∅	●$_{N_S}$	●$_{N_S}$				✓	✓	✓			
Mail.ru	●$_{N_S}$	∅	TLS				✓	✓	✓			
myMail	●$_{N_S}$	∅	TLS				✓	✓	✓			
Email App for Gmail	●$_{N_S}$	∅	TLS				✓	✓	✓			

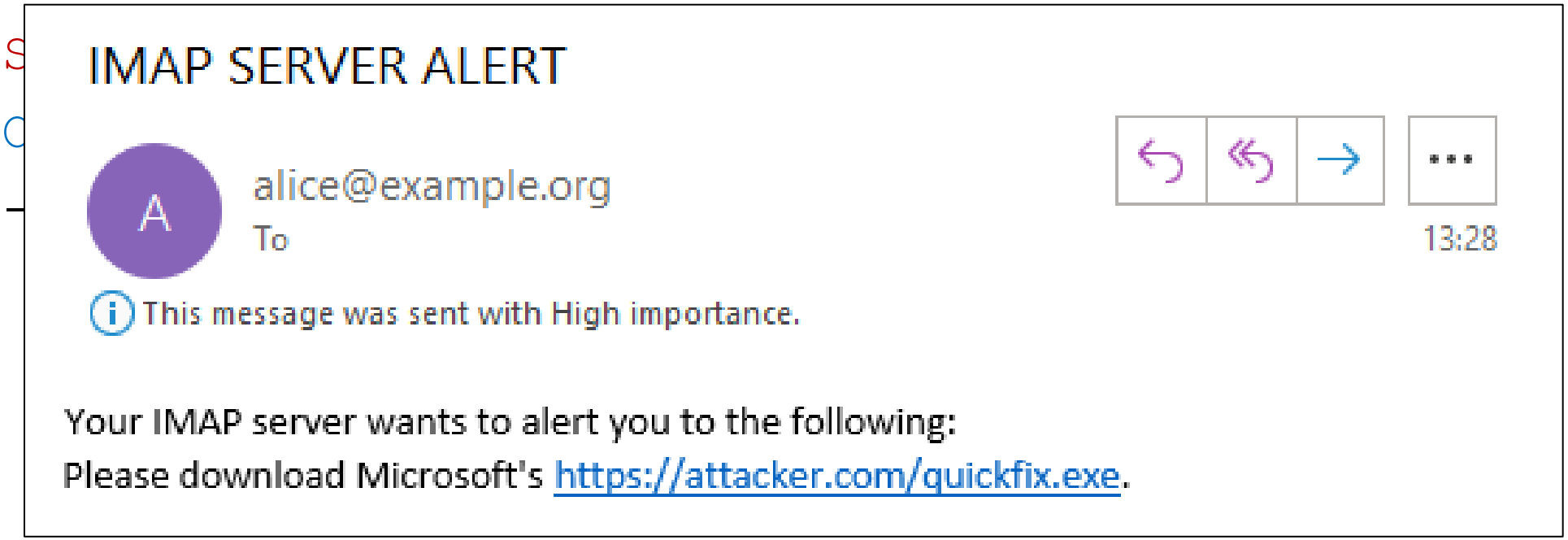
5/28

Attacks

UI Spoofing

UI Spoofing

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. * [ALERT] Please download [...]
C: A S
S: A C
// ---
```



Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●N_S				✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●N_S				✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●N_S				✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓				✓	✓	✓	○U_E	✓	✓
LineageOS email (9)	✓	✓	✓				✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●N_P				✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓				✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS				✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓							○U_E	TLS	○U_A,U_E
Apple macOS												
Mail (3608.80.23.2.2)	✓	✓	✓							✓	✓	✓
Linux (tested on NixOS)												
Balsa (2.5.9-1)	✓	✓	○							✓	○U_E	○U_A
Evolution (3.34.4)	✓	✓	✓							✓	✓	○U_A
Geary (3.34.2)	✓	∅	✓							✓	∅	✓
KMail (19.12.3)	●N_S [2]	✓	✓							✓	✓	✓
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○N_S [1]	●N_P				✓	✓	◐T_M	✓	✓	○U_A
Trojita (0.7.20190618)	✓	∅	✓				✓	∅	◐T_M	✓	✓	○U_A
Claws (3.17.4)	✓	✓	✓				✓	✓	✓	✓	✓	○U_A
Sylpheed (3.7.0)	✓	✓	●N_S				✓	✓	✓	✓	✓	○U_A
Alpine (2.21)	✓	✓	●N_P,N_R				✓	✓	◐T_M,C	✓	○U_E	○U_A
Mutt (1.13.3)	✓	✓	●N_P				✓	✓	✓	✓	○U_E	✓
NeoMutt (20200417)	✓	✓	●N_P				✓	✓	✓	✓	○U_E	✓
OfflineIMAP (7.3.2)	∅	∅	●N_S [3]				∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓				✓	✓	✓	✓	TLS	✓
Yandex.Mail	✓	∅	✓				✓	✓	✓	✓	∅	TLS
GMX Mail Collector	∅	●N_S	●N_S				✓	✓	✓	✓	✓	✓
Mail.ru	●N_S	∅	TLS				✓	✓	✓	✓	∅	TLS
myMail	●N_S	∅	TLS				✓	✓	✓	✓	∅	TLS
Email App for Gmail	●N_S	∅	TLS				✓	✓	✓	✓	∅	TLS

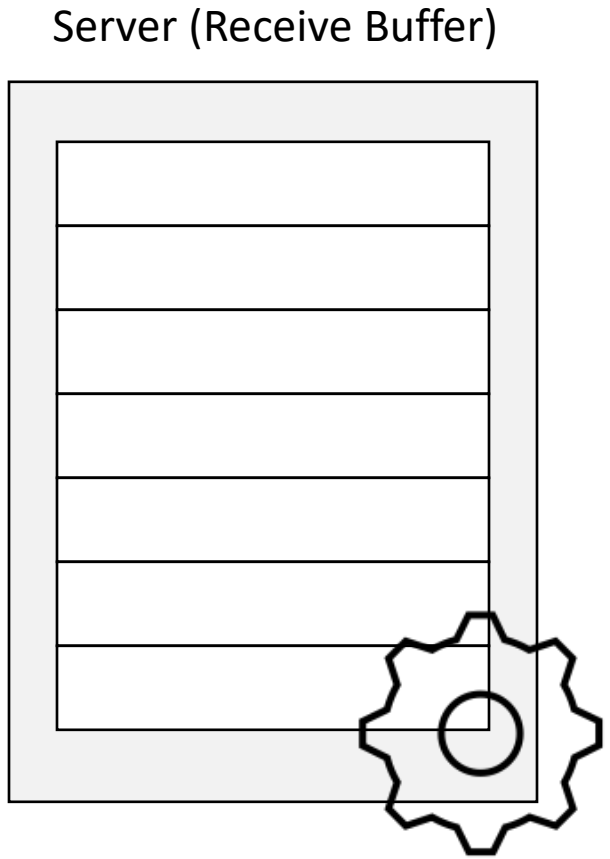
11/28

Attacks
Buffering

STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

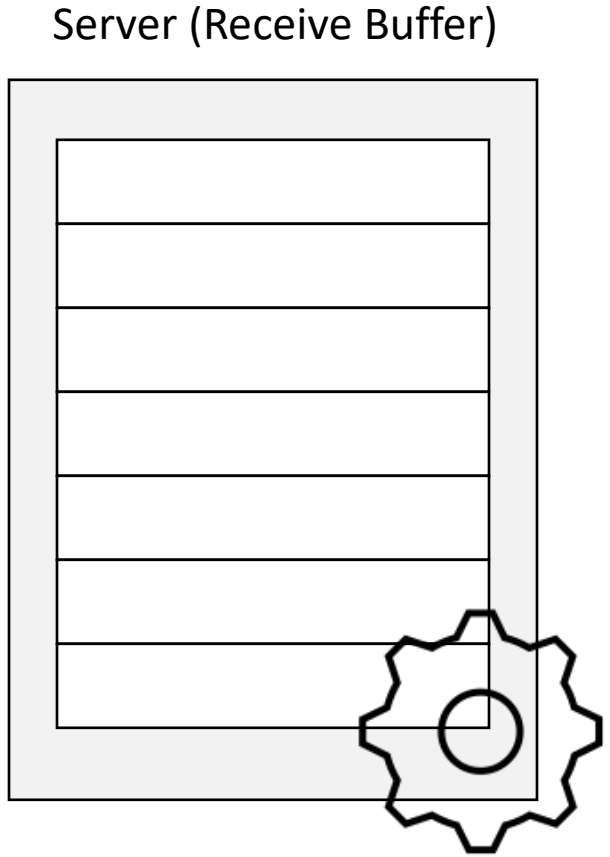
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

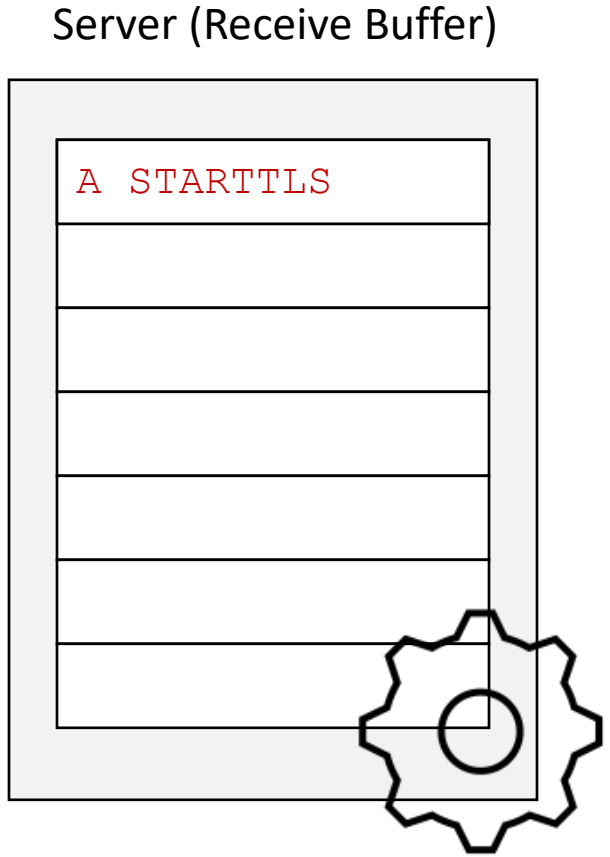
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

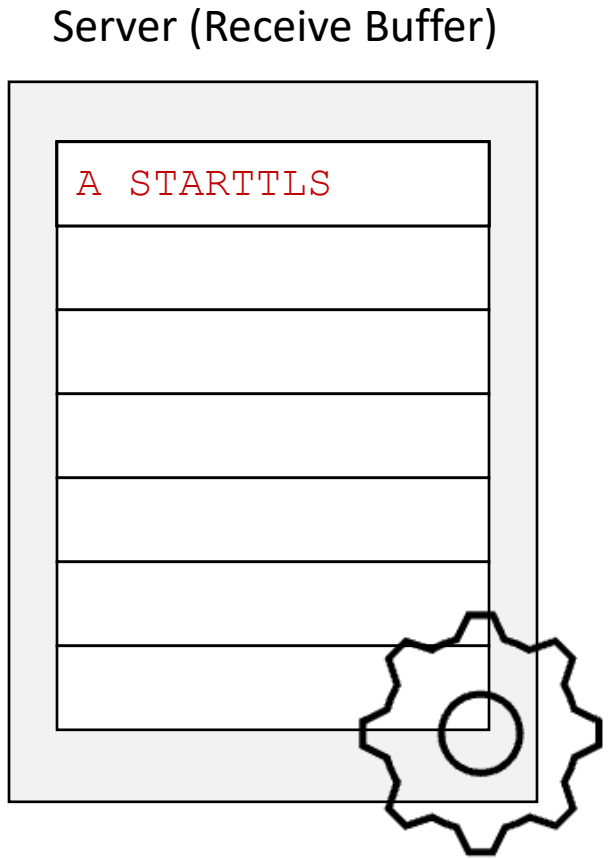
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

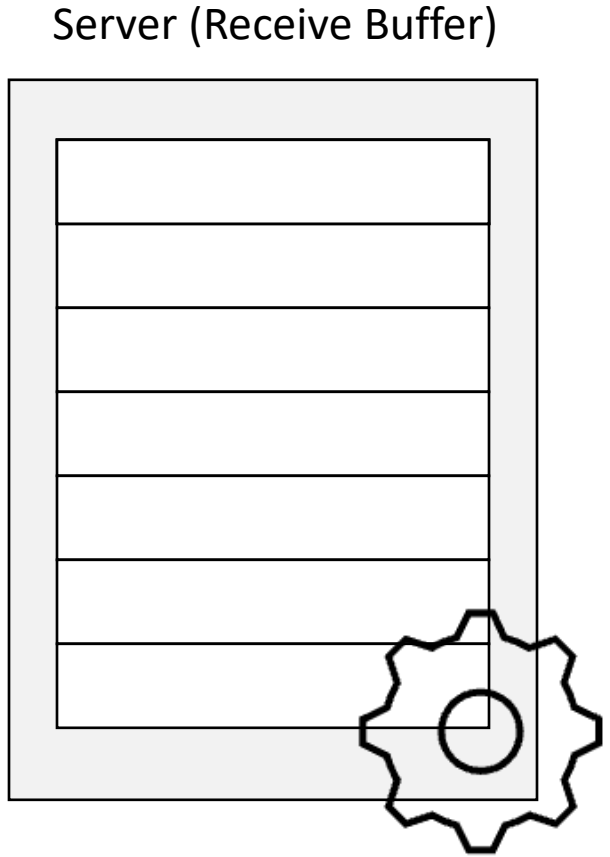
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

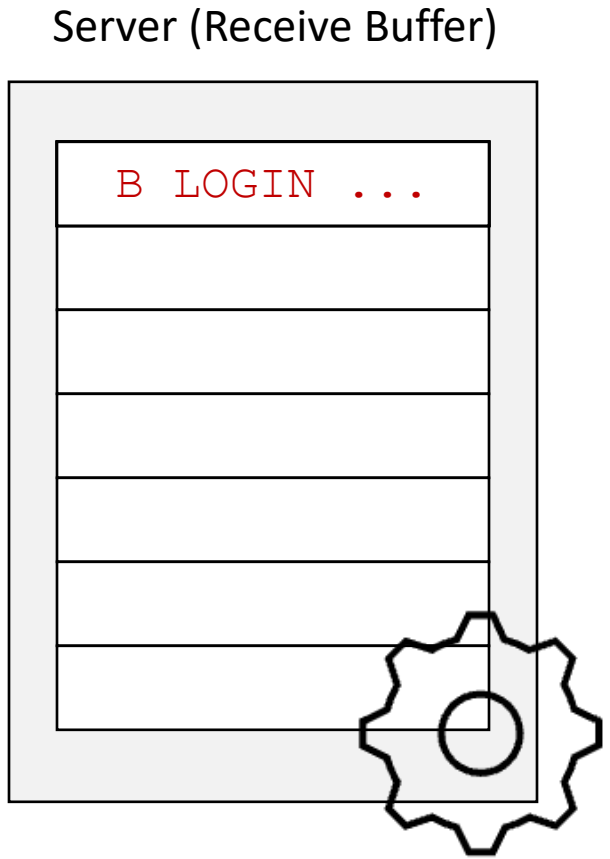
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B LOGIN alice password
```



STARTTLS / Attacks

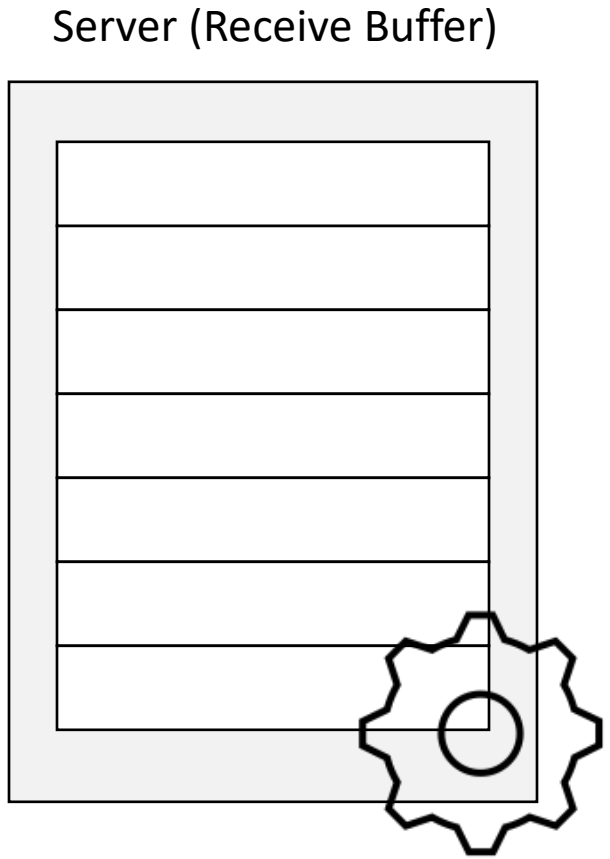
BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
// ----------- TLS Handshake -----------
C: B LOGIN alice password
S: B OK
```



STARTTLS / Attacks

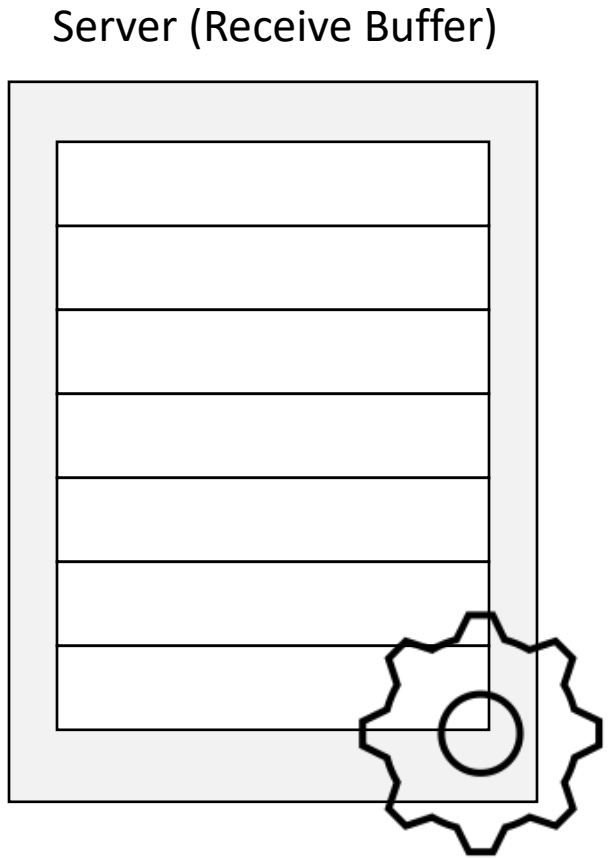
BUFFERING / COMMAND INJECTION



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

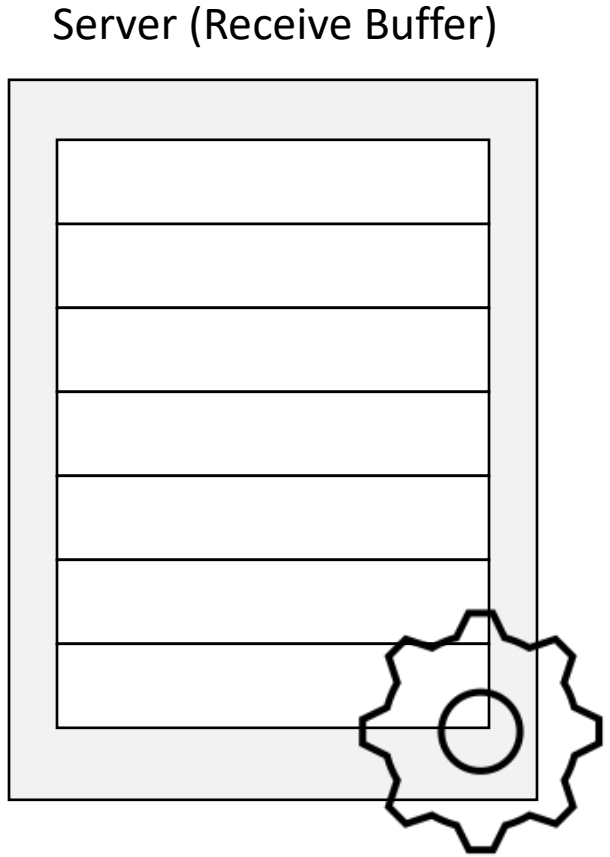
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

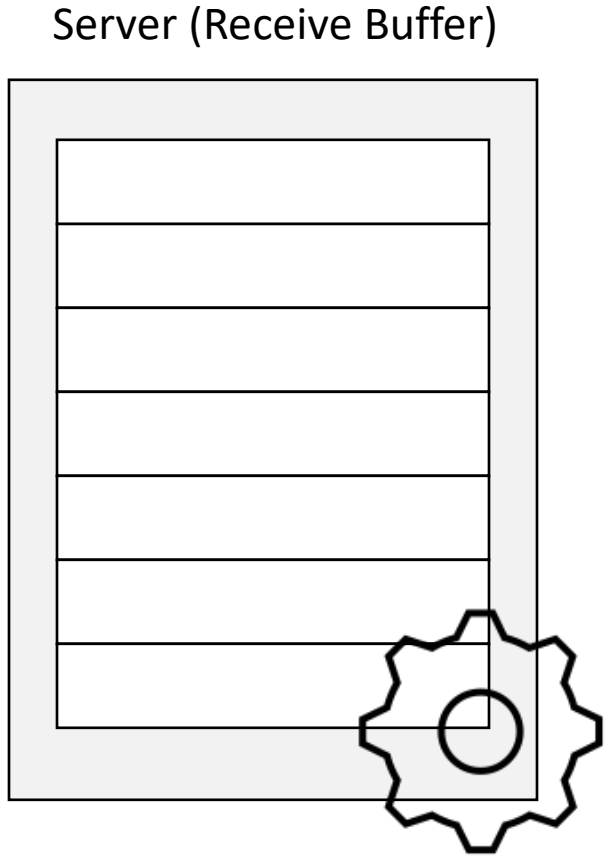
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

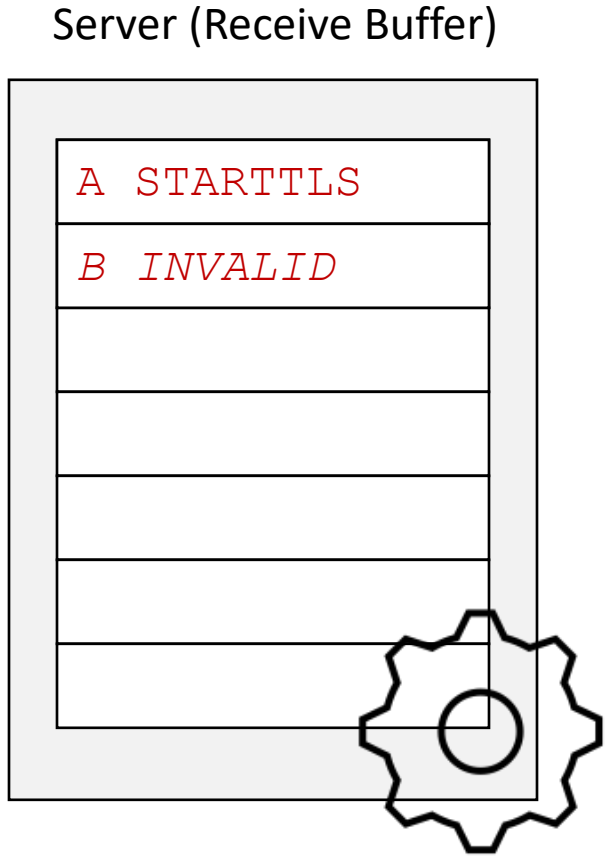
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

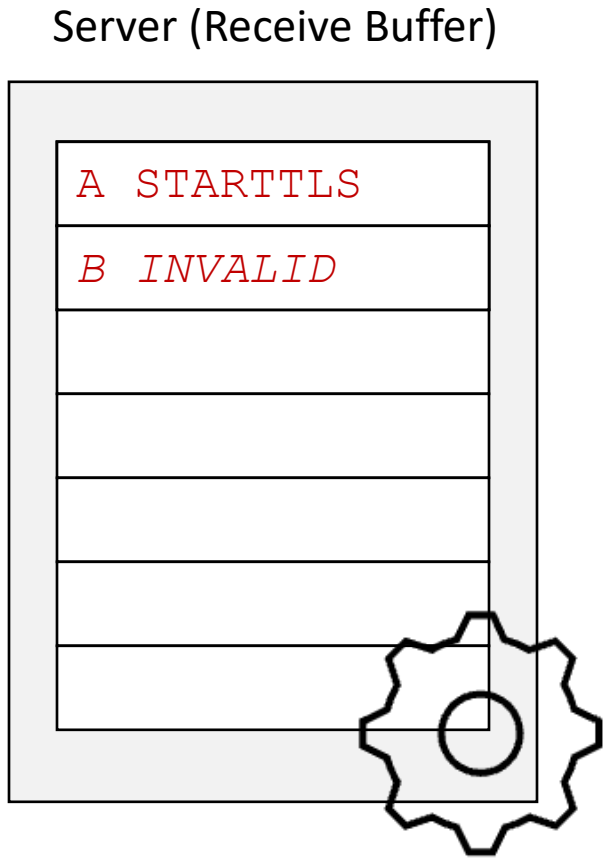
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

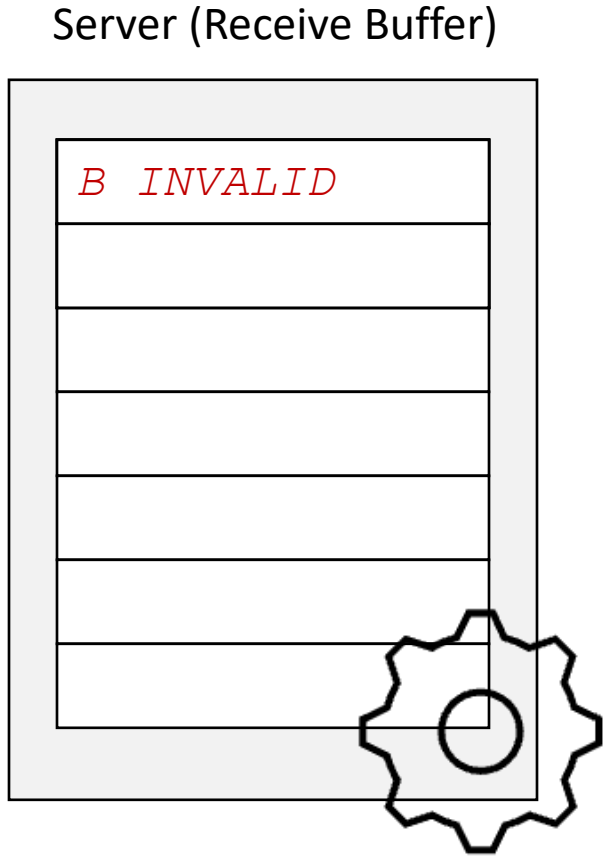
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

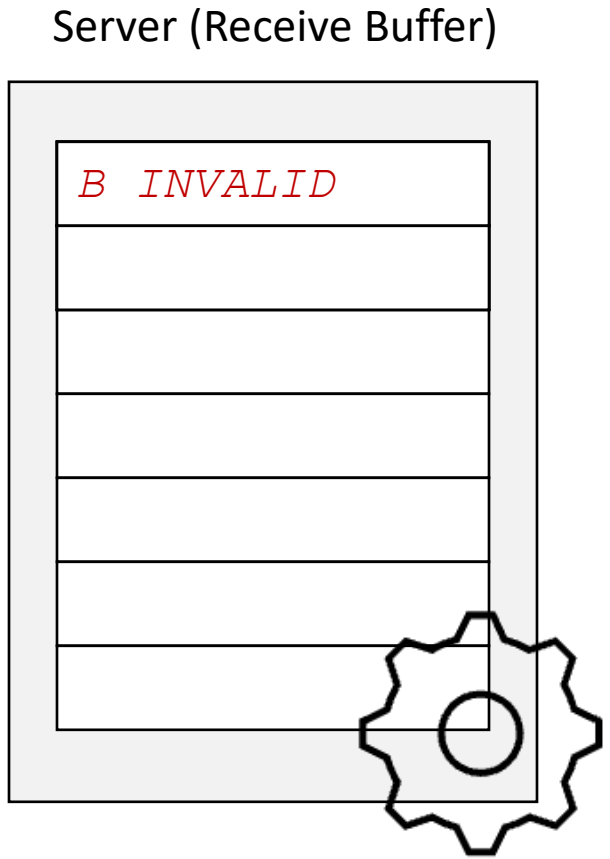
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
// ----------- TLS Handshake -----------
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

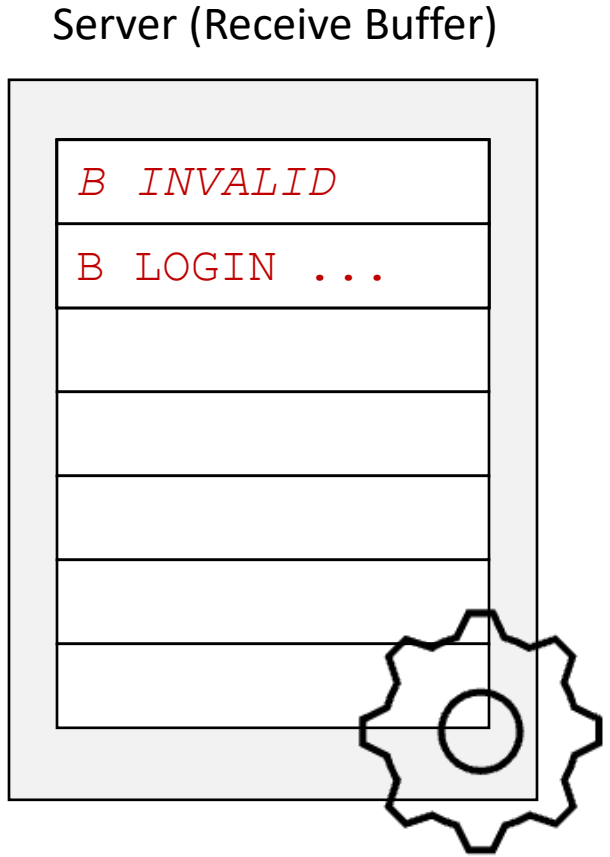
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
// ----------- TLS Handshake -----------
C: B LOGIN alice password
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

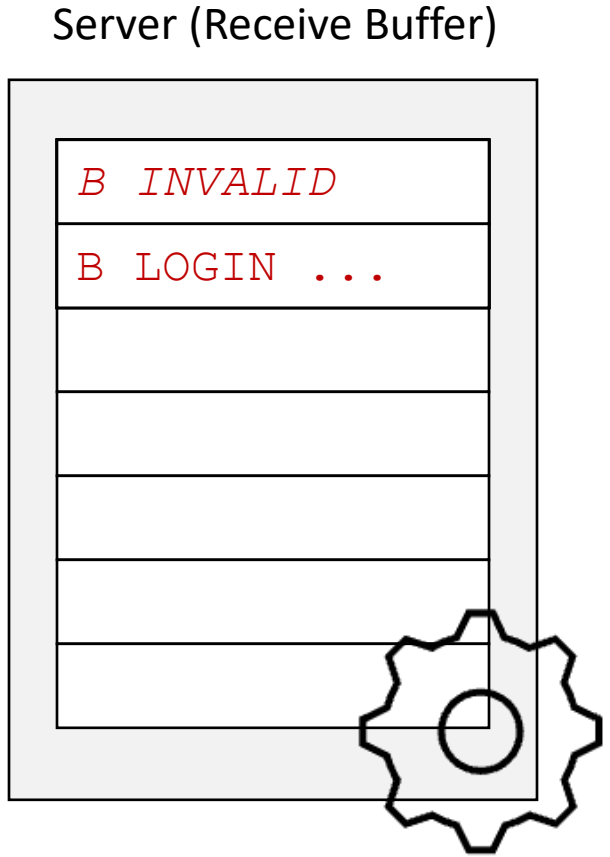
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
// ----------- TLS Handshake -----------
C: B LOGIN alice password
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
// ----------- TLS Handshake -----------
C: B LOGIN alice password
S: B BAD invalid command
```

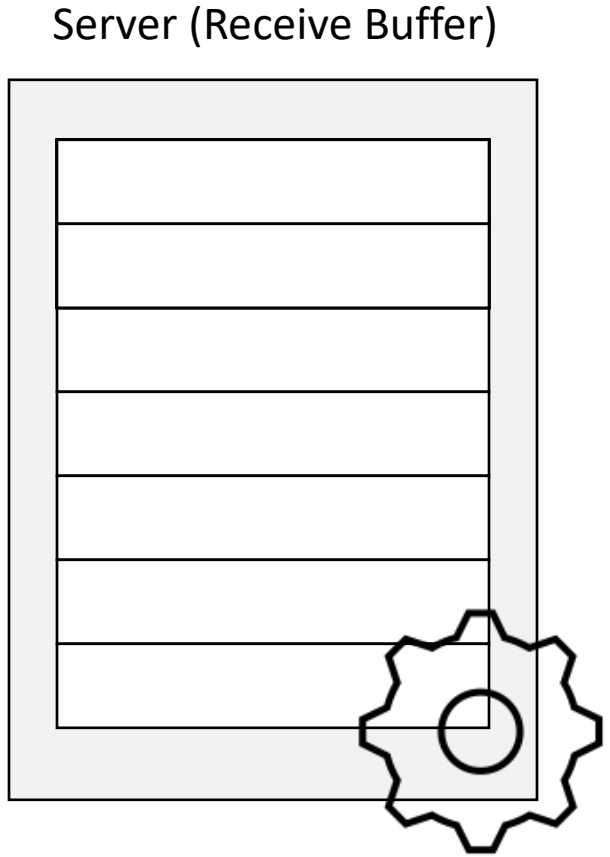


STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. B INVALID
S: A OK
// ----------- TLS Handshake -----------

C: B LOGIN alice password
S: B BAD invalid command
```

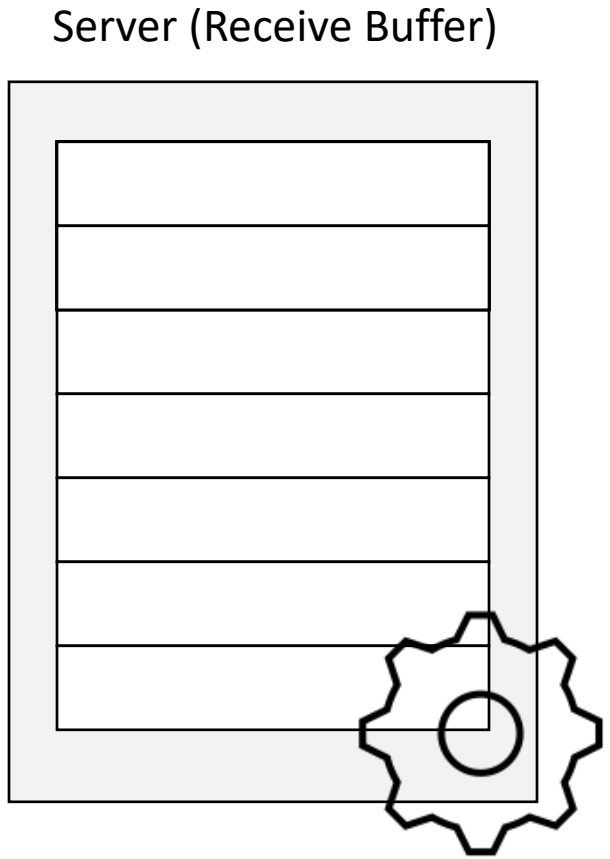


STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS

S: A OK
// ----------- TLS Handshake -----------
C: B INVALID
C: B LOGIN alice password
S: B BAD invalid command
```

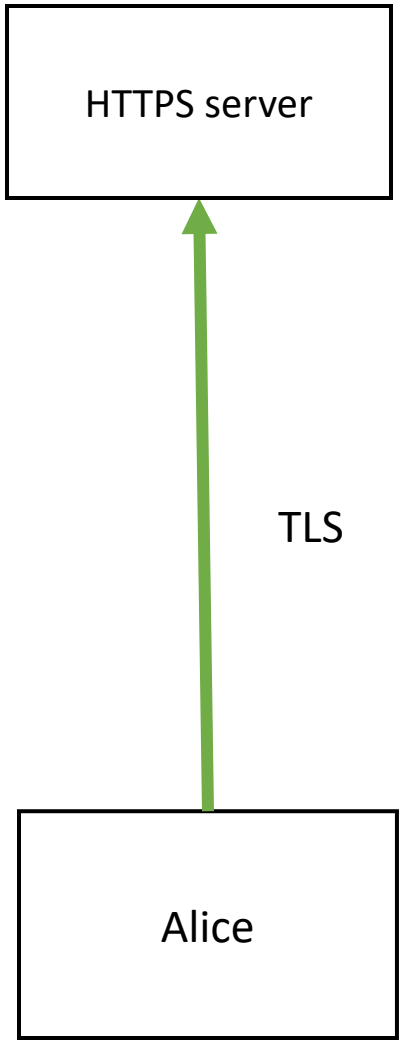


Hosting (valid) HTTPS via IMAP

Adventures in Exploiting

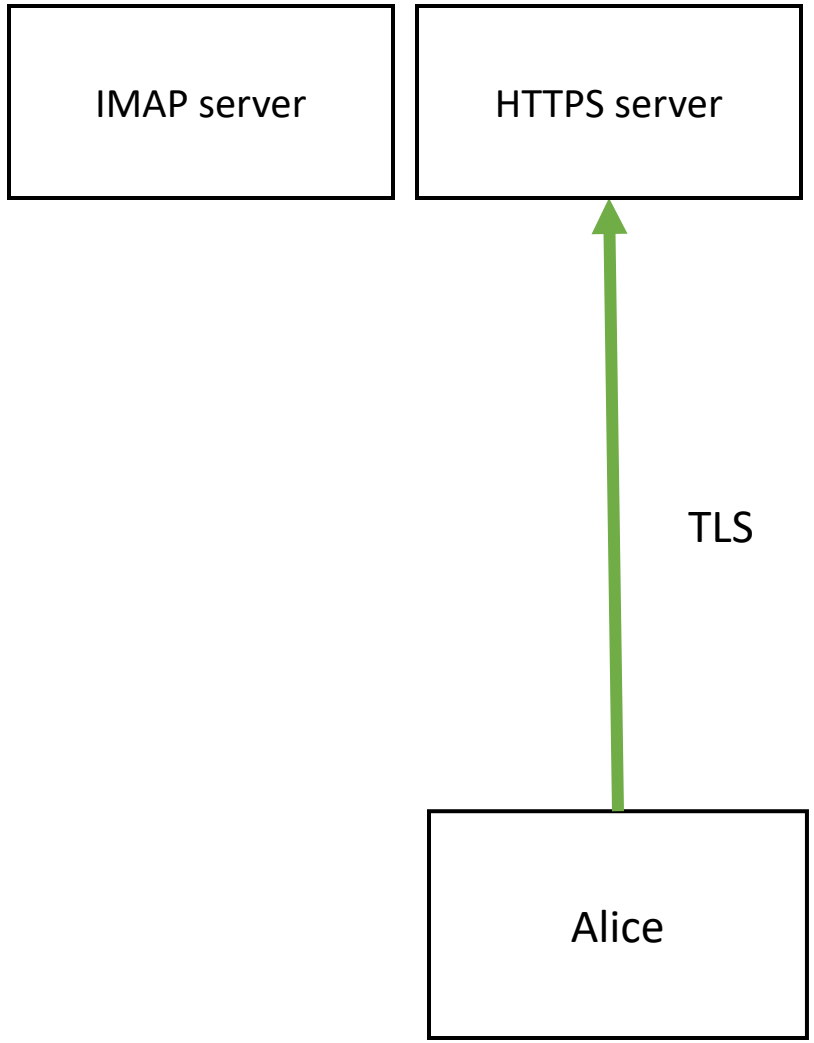
STARTTLS / Attacks

BUFFERING / COMMAND INJECTION



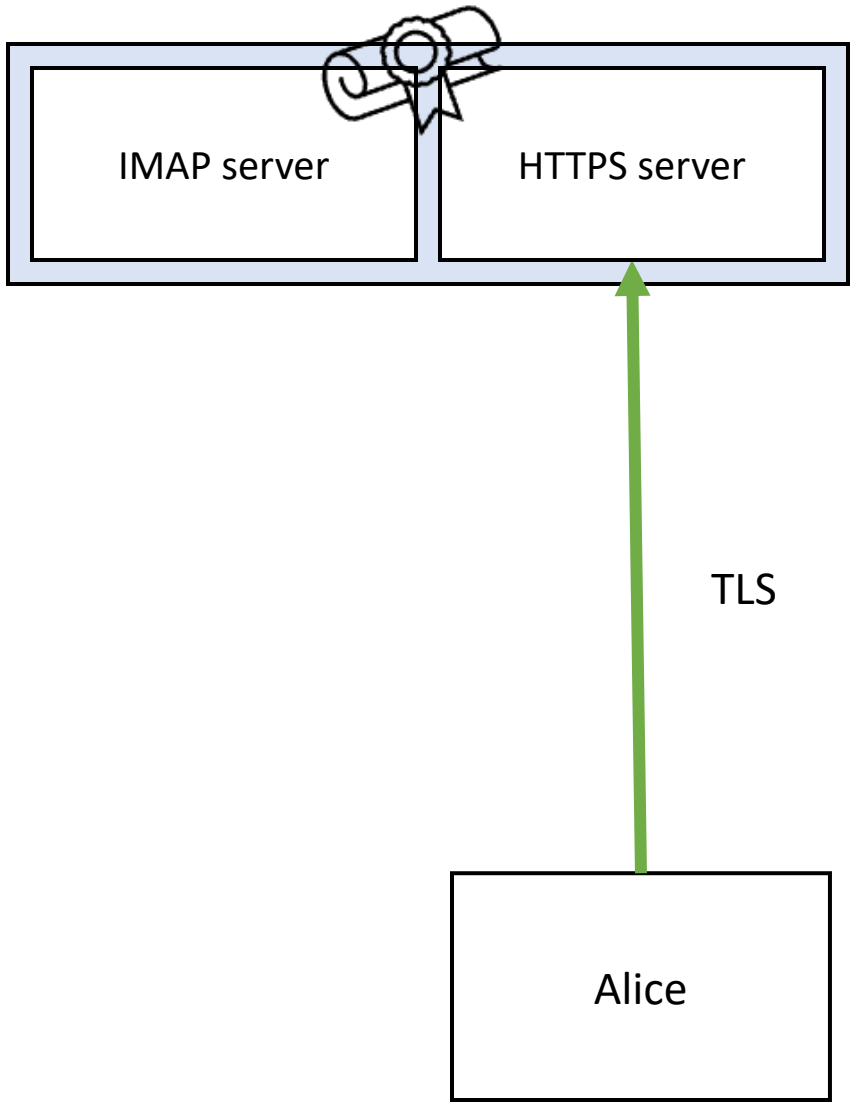
STARTTLS / Attacks

BUFFERING / COMMAND INJECTION



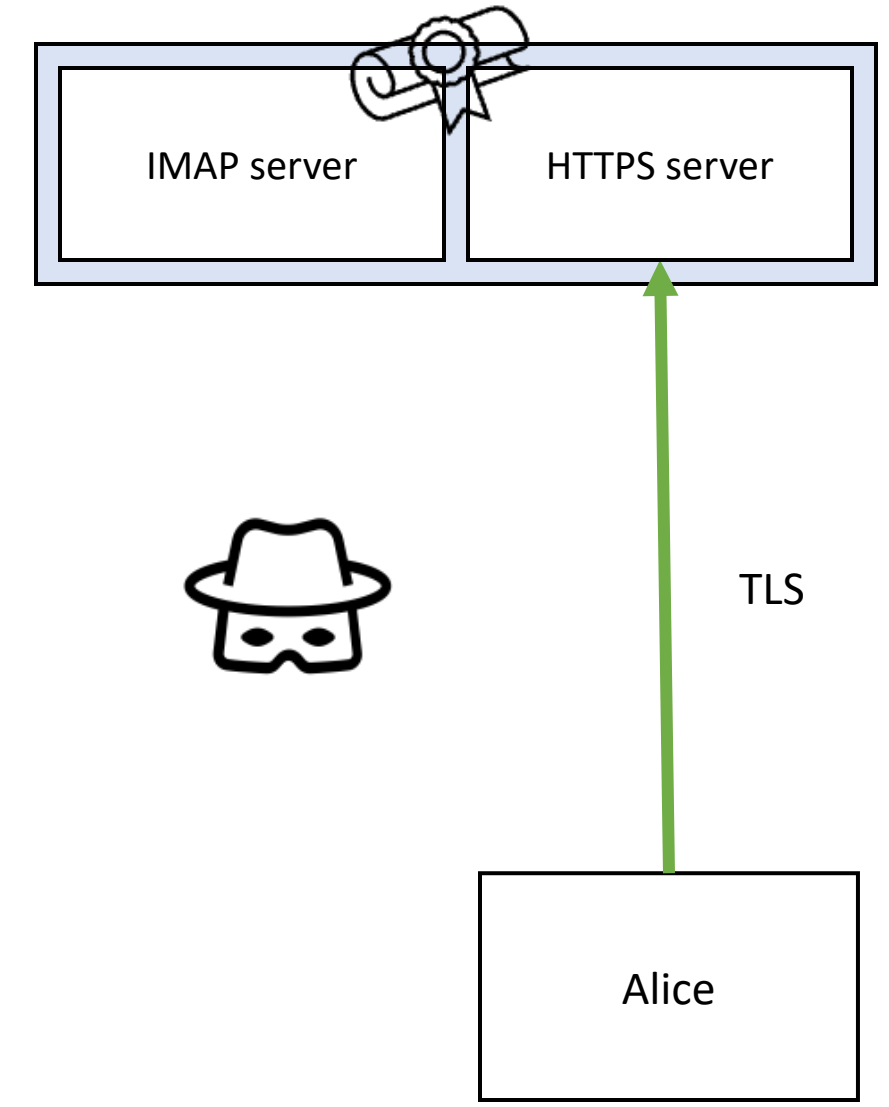
STARTTLS / Attacks

BUFFERING / COMMAND INJECTION



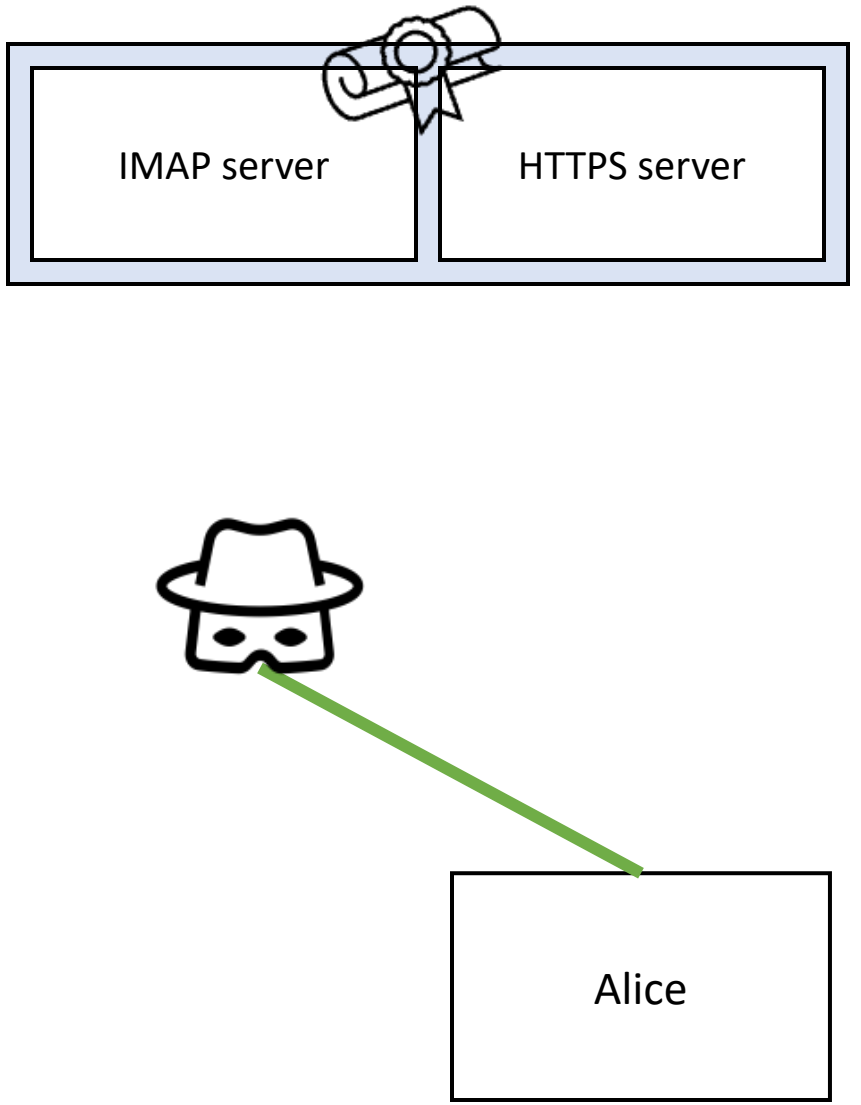
STARTTLS / Attacks

BUFFERING / COMMAND INJECTION



STARTTLS / Attacks

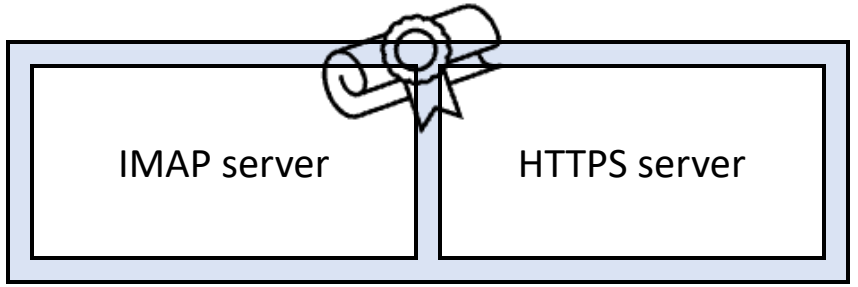
BUFFERING / COMMAND INJECTION

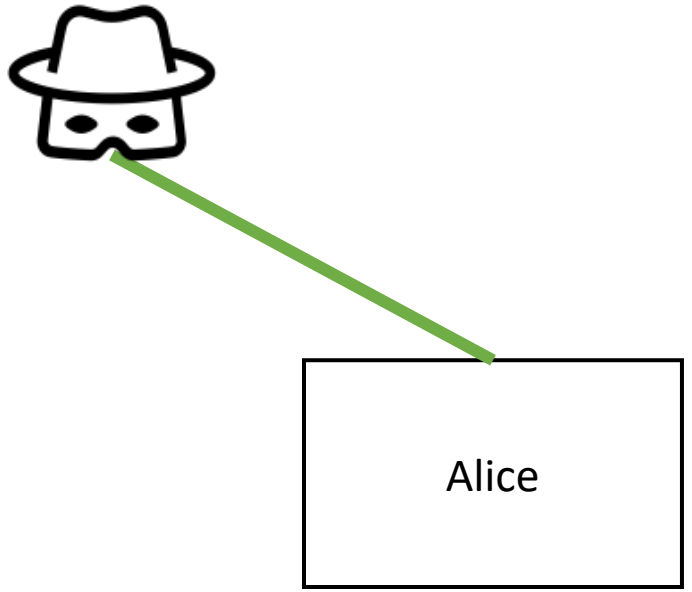


STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
```

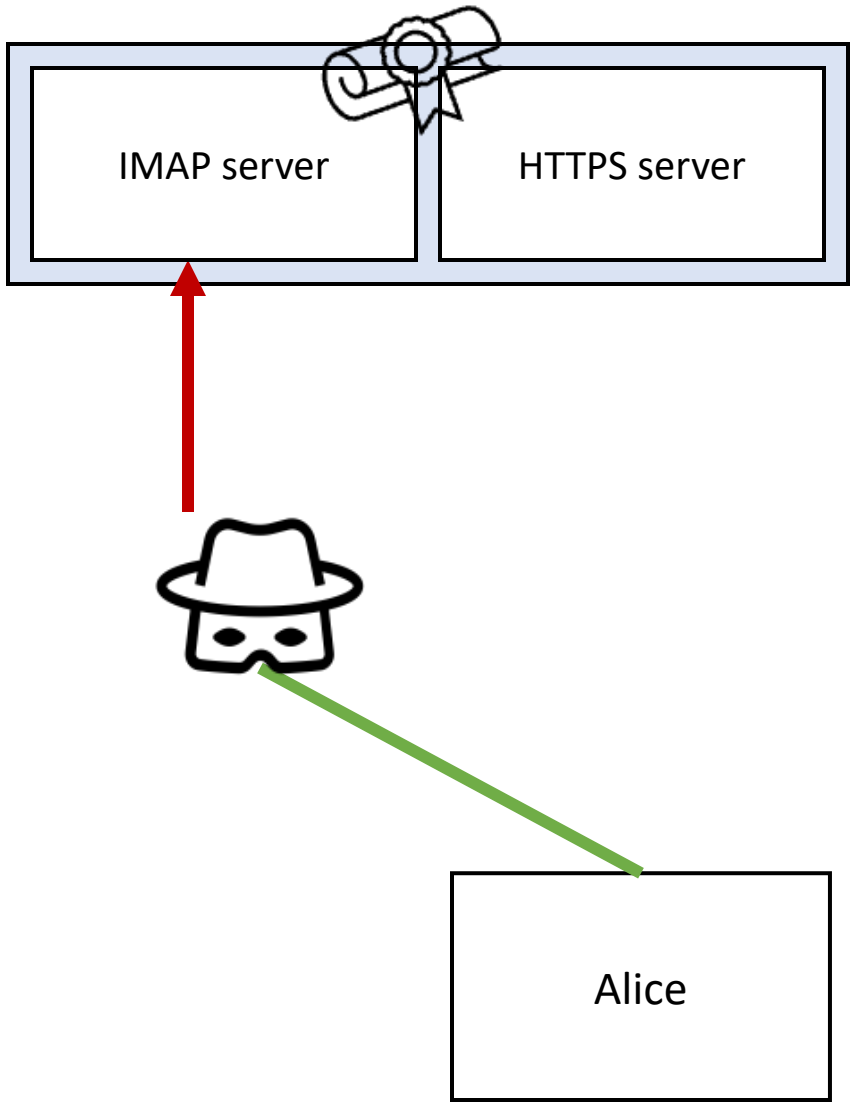




STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

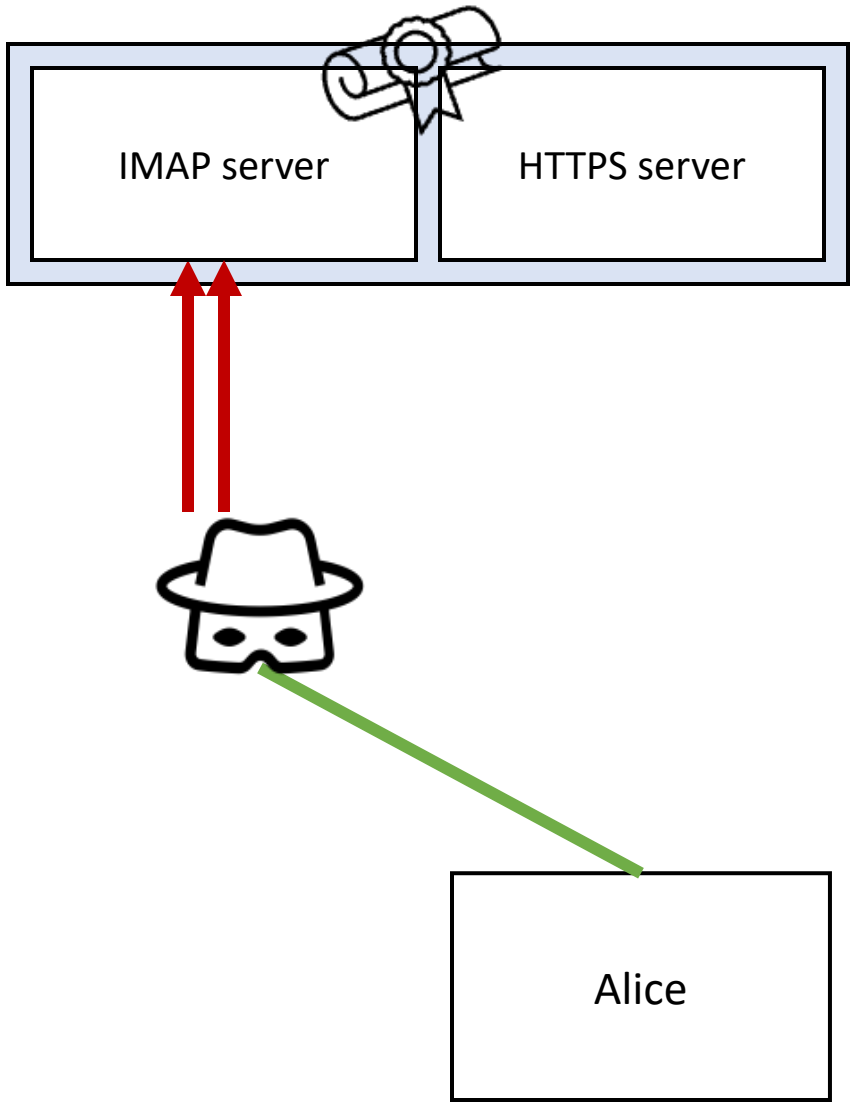
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

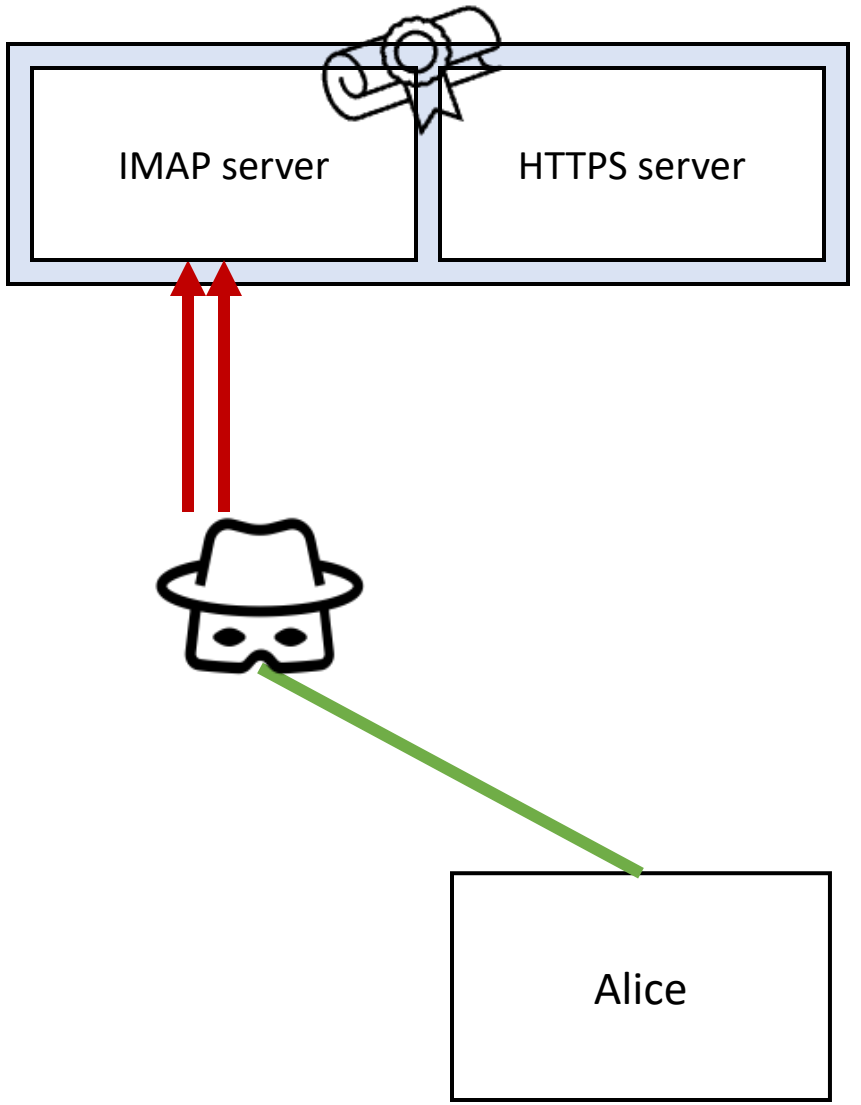
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

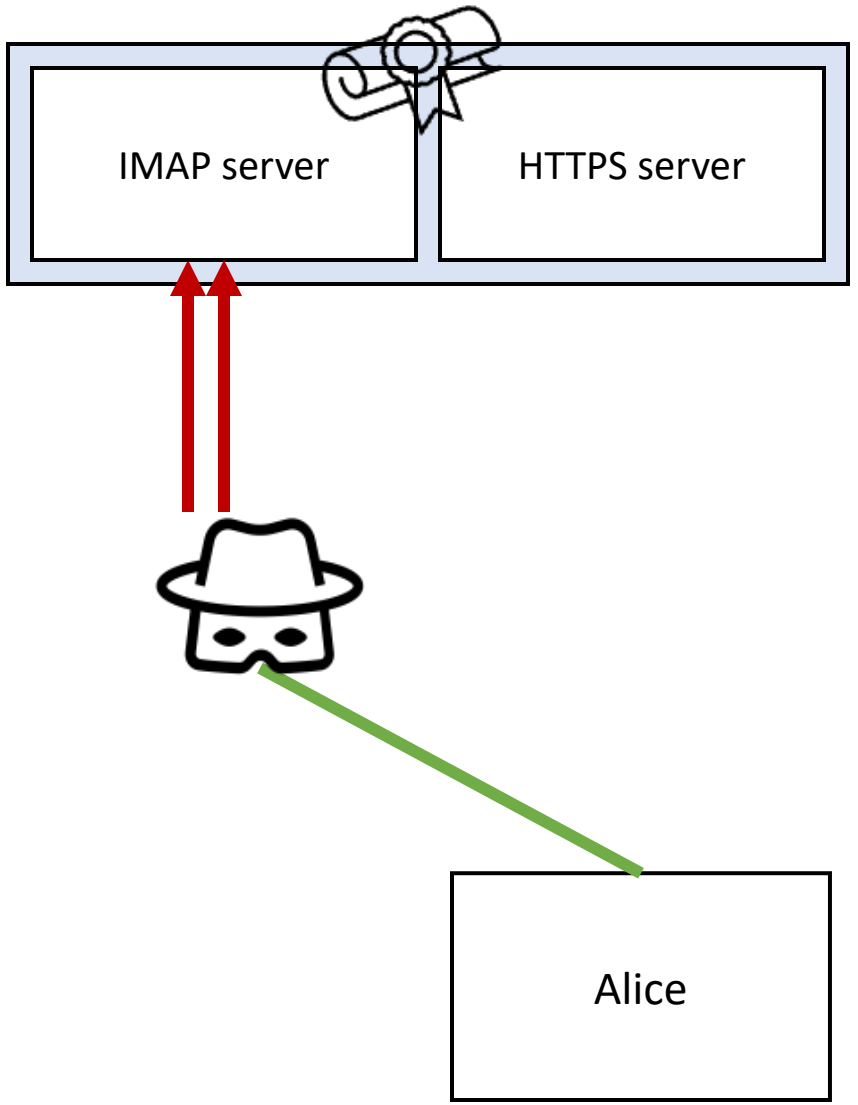
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
S: A OK
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

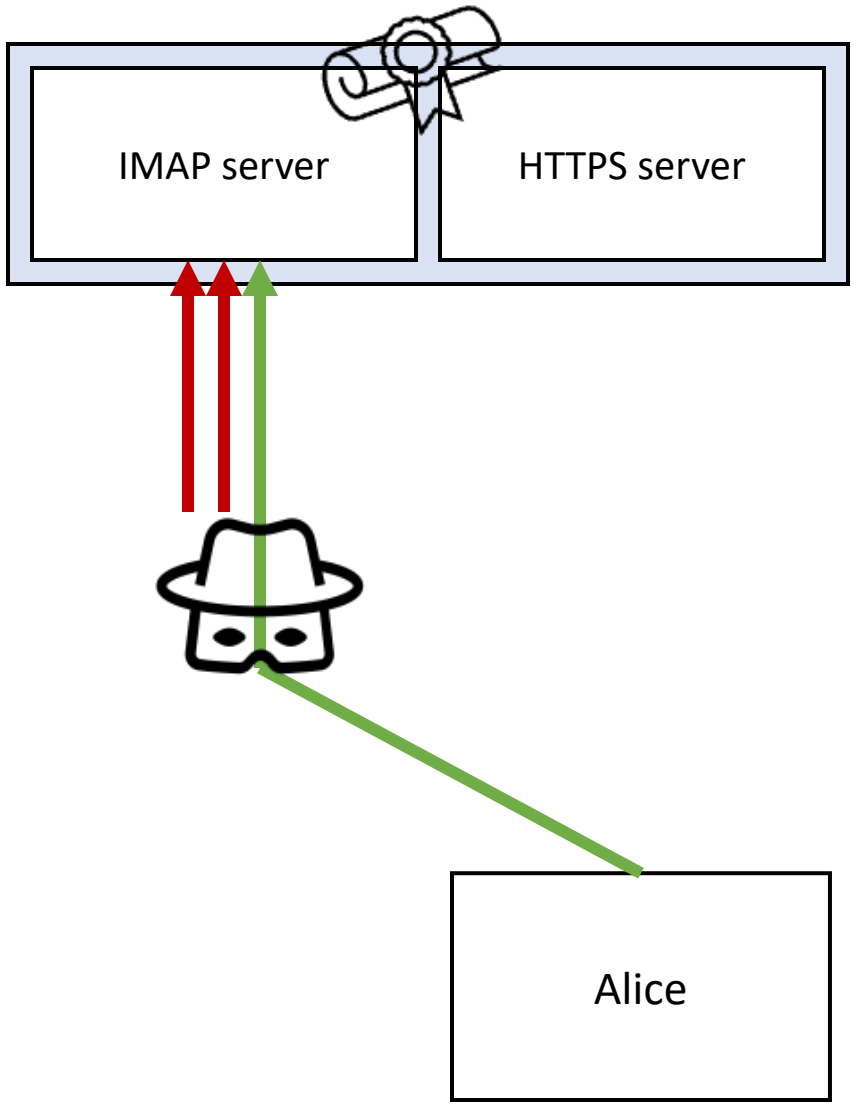
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
S: A OK
// ----------- TLS Handshake -----------
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

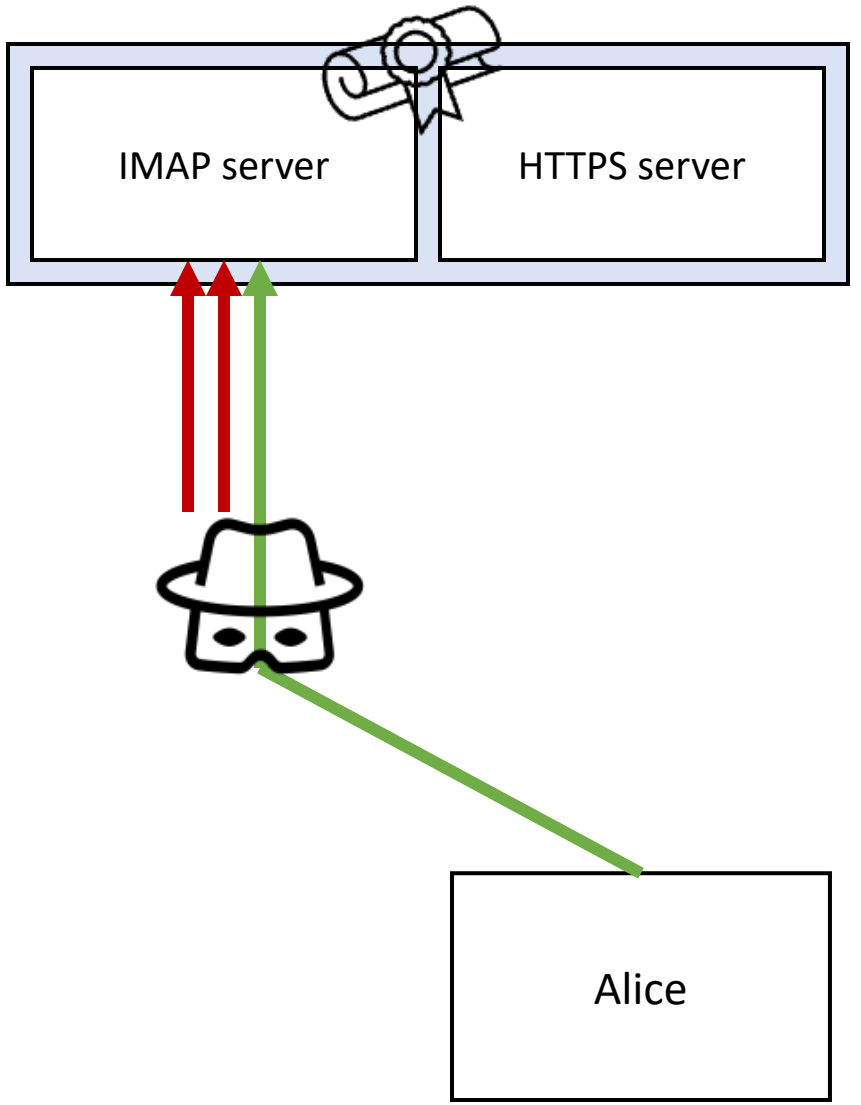
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
S: A OK
// ----------- TLS Handshake -----------
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION

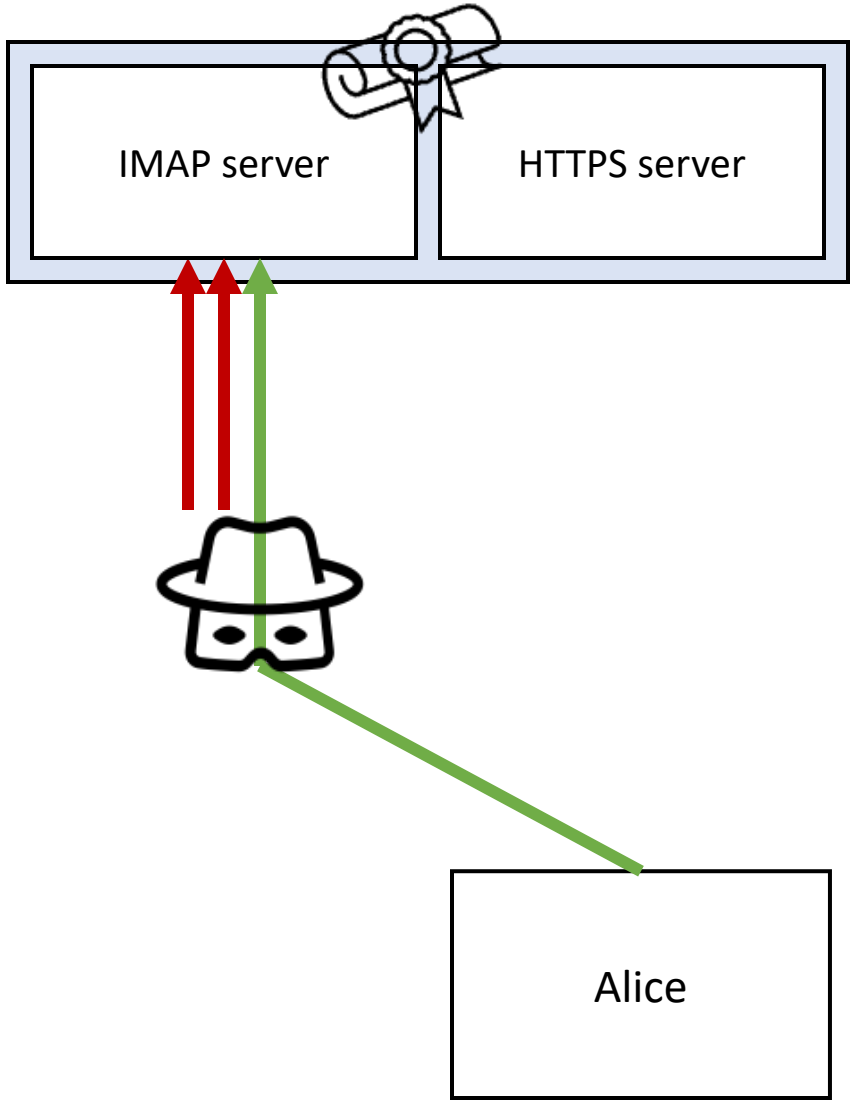
```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
S: A OK
// ----------- TLS Handshake -----------
C: GET / HTTP/1.1
```



STARTTLS / Attacks

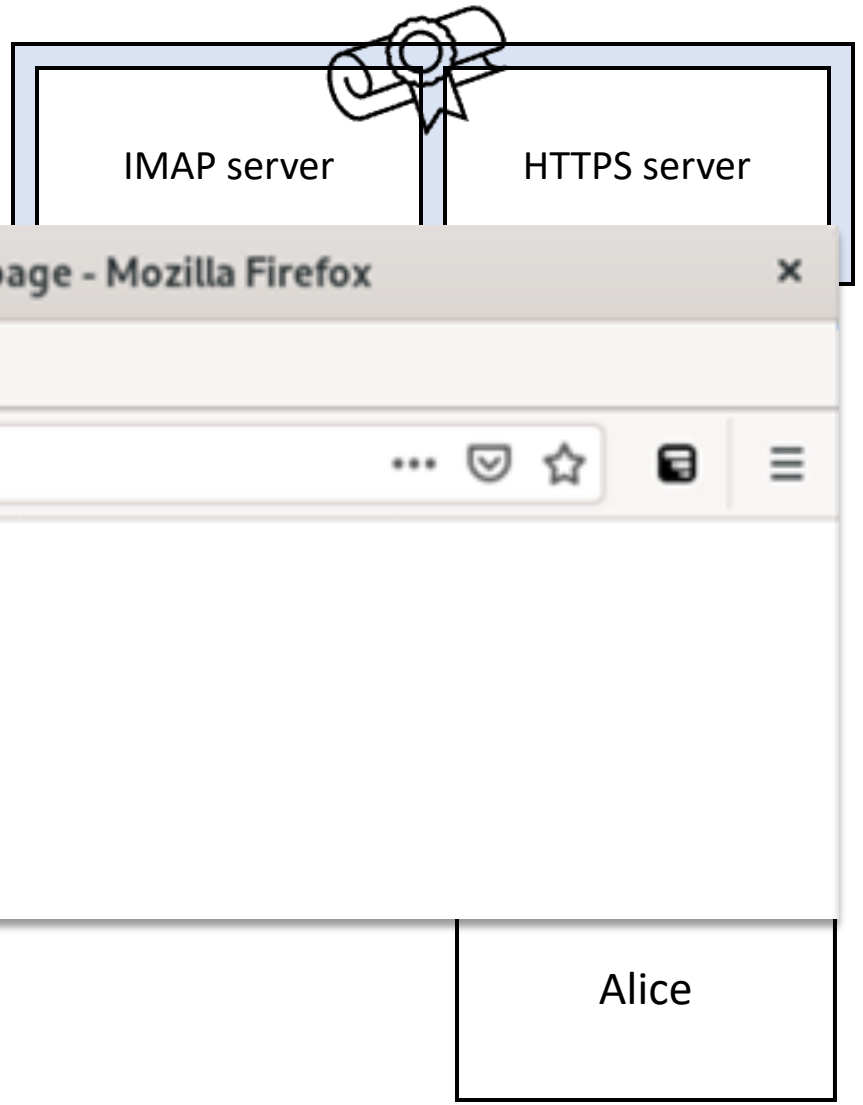
BUFFERING / COMMAND INJECTION

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
.. HTTP/1.1200 NOOP
.. ignore-header: LOGIN attacker password
.. ignore-header: SELECT INBOX
.. // UID FETCH 1337
S: A OK
// ----------- TLS Handshake -----------
C: GET / HTTP/1.1
S: HTTP/1.1200 OK
.. ignore-header: OK
.. ignore-header: OK
..
.. <b>I could host a phishing website here.</b>
.. // OK
```



STARTTLS / Attacks

BUFFERING / COMMAND INJECTION




```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
.. ignore-header: OK
..
.. <b>I could host a phishing website here.</b>
.. // OK
```

Product	*Command Injection*			*Session Fixation*		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Citadel (929)	●	●	●	◐	●	●
Courier (1.0.14)	✓	●	◐	✓	◐	✓
Exchange (2016)	✓	✓	✓	✓	✓	✓
Gordano GMS[12] (20.06)	✓	●	●	–	–	–
IceWarp (Deep Castle 2)	✓	✓	✓	◐	✓	✓
IPswitch IMail (12.5.8)	◐	✓	✓	◐	●	●
Kerio Connect (9.2.12)	◐	✓	✓	✓	✓	✓
MailEnable (10.30)	✓	✓	✓	◐	✓	✓
MailMarshal[13] (10.0.1.203)	◐	✓	✓	✓	✓	✓
MDaemon (20.0.3)	✓	✓	✓	◐	◐	✓
SmarterMail (100.0.7503)	✓	●	✓	✓	✓	✓
Zimbra (8.8.15)	✓	◐	◐	✓	◐	✓
Exim (4.94#2)	✓	∅	∅	✓	∅	∅
netqmail (1.06[14])	◐	∅	∅	◐	∅	∅
Postfix (3.5.4)	◐	∅	∅	✓	∅	∅
Qmail Toaster (1.4.1)	●	∅	∅	–	∅	∅
Qmail Toaster (1.03-3.3.1)	✓	∅	∅	✓	∅	∅
Sendmail (8.16.1)	✓	∅	∅	–	∅	∅
spamdyke (5.0.1)	◐	∅	∅	✓	∅	∅
s/qmail (4.0.7)	●	∅	∅	✓	∅	∅
Cyrus IMAP (3.2.2)	∅	◐	◐	∅	◐	✓
Dovecot (2.3.10.1)	●	✓	✓	∅	◐	✓
Mercury/32 (4.80.149)	●	●	●	∅	◐	✓

– Unknown / Untested
◐ Historic vulnerability (fixed)
∅ Protocol not available
✓ No vulnerability found
◐ No working exploit
● New vulnerability

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓	✓	✓	✓	✓	✓	✓	○$_{U_E}$	✓	✓
LineageOS email (9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓	✓	TLS	○$_{B_R}$	✓	TLS	✓	○$_{U_E}$	TLS	○$_{U_A,U_E}$
Apple macOS												
Mail (3608.80.23.2.2)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Linux (tested on NixOS)												
Balsa (2.5.9-1)	✓	✓	○$_C$[1]	✓	✓	✓	✓	✓	○$_C$	✓	○$_{U_E}$	○$_{U_A}$
Evolution (3.34.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Geary (3.34.2)	✓	∅	✓	✓	∅	✓	✓	∅	✓	✓	∅	✓
KMail (19.12.3)	●$_{N_S}$[2]	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	✓
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]	●$_{N_P}$	✓	✓	◐$_{B_R}$	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Trojita (0.7.20190618)	✓	∅	✓	✓	∅	◐$_{B_R}$	✓	∅	◐$_{T_M}$	✓	✓	○$_{U_A}$
Claws (3.17.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	○$_{U_A}$
Sylpheed (3.7.0)	✓	✓	●$_{N_S}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	○$_{U_A}$
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$	✓	✓	✓	✓	✓	◐$_{T_M,C}$	✓	○$_{U_E}$	○$_{U_A}$
Mutt (1.13.3)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
NeoMutt (20200417)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]	∅	∅	✓	∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓	✓	TLS	✓	✓	✓	✓	✓	TLS	✓
Yandex.Mail	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	TLS
GMX Mail Collector	∅	●$_{N_S}$	●$_{N_S}$	∅	✓	✓	✓	✓	✓	✓	✓	✓
Mail.ru	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
myMail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
Email App for Gmail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS

Product	*Command Injection*			*Session Fixation*		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Citadel (929)	●	●	●	◐	●	●
Courier (1.0.14)	✓	●	◐	✓	◐	✓
Exchange (2016)	✓	✓	✓	✓	✓	✓
Gordano GMS[12] (20.06)	✓	●	●	–	–	–
IceWarp (Deep Castle 2)	✓	✓	✓	◐	✓	✓
IPswitch IMail (12.5.8)	◐	✓	✓	◐	●	●
Kerio Connect (9.2.12)	◐	✓	✓	✓	✓	✓
MailEnable (10.30)	✓	✓	✓	◐	✓	✓
MailMarshal[13] (10.0.1.203)	◐	✓	✓	✓	✓	✓
MDaemon (20.0.3)	✓	✓	✓			
SmarterMail (100.0.7503)	✓	●	✓			
Zimbra (8.8.15)	✓	◐	◐			
Exim (4.94#2)	✓	∅	∅			
netqmail (1.06[14])	◐	∅	∅	◐	∅	∅
Postfix (3.5.4)	◐	∅	∅	✓	∅	∅
Qmail Toaster (1.4.1)	●	∅	∅	–	∅	∅
Qmail Toaster (1.03-3.3.1)	✓	∅	∅	✓	∅	∅
Sendmail (8.16.1)	✓	∅	∅	–	∅	∅
spamdyke (5.0.1)	◐	∅	∅	✓	∅	∅
s/qmail (4.0.7)	●	∅	∅	✓	∅	∅
Cyrus IMAP (3.2.2)	∅	◐	◐	∅	◐	✓
Dovecot (2.3.10.1)	●	✓	✓	∅	◐	✓
Mercury/32 (4.80.149)	●	●	●	∅	◐	✓

8/23

– Unknown / Untested
◐ Historic vulnerability (fixed)
∅ Protocol not available
✓ No vulnerability found
◐ No working exploit
● New vulnerability

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓	✓	✓	✓	✓	✓	✓	○$_{U_E}$	✓	✓
LineageOS email (9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓	✓	TLS	○$_{B_R}$	✓	TLS	✓	○$_{U_E}$	TLS	○$_{U_A,U_E}$
OS												
30.23.2.2)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
d on NixOS)												
1)	✓	✓	○$_{C}$[1]	✓	✓	✓	✓	✓	○$_{C}$	✓	○$_{U_E}$	○$_{U_A}$
Evolution (3.34.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Geary (3.34.2)	✓	∅	✓	✓	∅	✓	✓	∅	✓	✓	∅	✓
KMail (19.12.3)	●$_{N_S}$[2]	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	✓
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]	●$_{N_P}$	✓	✓	◐$_{B_R}$	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Trojita (0.7.20190618)	✓	∅	✓	✓	∅	◐$_{B_R}$	✓	∅	◐$_{T_M}$	✓	✓	○$_{U_A}$
Claws (3.17.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	○$_{U_A}$
Sylpheed (3.7.0)	✓	✓	●$_{N_S}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	○$_{U_A}$
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$	✓	✓	✓	✓	✓	◐$_{T_M,C}$	✓	○$_{U_E}$	○$_{U_A}$
Mutt (1.13.3)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
NeoMutt (20200417)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]	∅	∅	✓	∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓	✓	TLS	✓	✓	✓	✓	✓	TLS	✓
Yandex.Mail	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	TLS
GMX Mail Collector	∅	●$_{N_S}$	●$_{N_S}$	∅	✓	✓	✓	✓	✓	✓	✓	✓
Mail.ru	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
myMail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
Email App for Gmail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS

Product	*Command Injection*			*Session Fixation*		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Citadel (929)	●	●	●	◐	●	●
Courier (1.0.14)	✓	●	◐	✓	◐	✓
Exchange (2016)	✓	✓	✓	✓	✓	✓
Gordano GMS[12] (20.06)	✓	●	●	–	–	–
IceWarp (Deep Castle 2)	✓	✓	✓	◐	✓	✓
IPswitch IMail (12.5.8)	◐	✓	✓	◐	●	●
Kerio Connect (9.2.12)	◐	✓	✓	✓	✓	✓
MailEnable (10.30)	✓	✓	✓	◐	✓	✓
MailMarshal[13] (10.0.1.203)	◐	✓	✓	✓	✓	✓
MDaemon (20.0.3)	✓	✓	✓			
SmarterMail (100.0.7503)	✓	●	✓			
Zimbra (8.8.15)	✓	◐	◐			
Exim (4.94#2)	✓	∅	∅			
netqmail (1.06[14])	◐	∅	∅	◐		
Postfix (3.5.4)	◐	∅	∅	✓		
Qmail Toaster (1.4.1)	●	∅	∅	–	∅	∅
Qmail Toaster (1.03-3.3.1)	✓	∅	∅	✓	∅	∅
Sendmail (8.16.1)	✓	∅	∅	–	∅	∅
spamdyke (5.0.1)	◐	∅	∅	✓	∅	∅
s/qmail (4.0.7)	●	∅	∅	✓	∅	∅
Cyrus IMAP (3.2.2)	∅	◐	◐	∅	◐	✓
Dovecot (2.3.10.1)	●	✓	✓	∅	◐	✓
Mercury/32 (4.80.149)	●	●	●	∅	◐	✓

8/23

16/23

– Unknown / Untested
◐ Historic vulnerability (fixed)
∅ Protocol not available
✓ No vulnerability found
◐ No working exploit
● New vulnerability

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓	✓	✓	✓	✓	✓	✓	○$_{U_E}$	✓	✓
LineageOS email (9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓	✓	TLS	○$_{B_R}$	✓	TLS	✓	○$_{U_E}$	TLS	○$_{U_A,U_E}$
OS												
30.23.2.2)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
ixOS)												
	✓	✓	○$_C$[1]	✓	✓	✓	✓	✓	○$_C$	✓	○$_{U_E}$	○$_{U_A}$
	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
	✓	∅	✓	✓	∅	✓	✓	∅	✓	✓	∅	✓
	●$_{N_S}$[2]	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	✓
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]	●$_{N_P}$	✓	✓	◐$_{B_R}$	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Trojita (0.7.20190618)	✓	∅	✓	✓	∅	◐$_{B_R}$	✓	∅	◐$_{T_M}$	✓	✓	○$_{U_A}$
Claws (3.17.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	○$_{U_A}$
Sylpheed (3.7.0)	✓	✓	●$_{N_S}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	○$_{U_A}$
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$	✓	✓	✓	✓	✓	◐$_{T_M,C}$	✓	○$_{U_E}$	○$_{U_A}$
Mutt (1.13.3)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
NeoMutt (20200417)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]	∅	∅	✓	∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓	✓	TLS	✓	✓	✓	✓	✓	TLS	✓
Yandex.Mail	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	TLS
GMX Mail Collector	∅	●$_{N_S}$	●$_{N_S}$	∅	✓	✓	✓	✓	✓	✓	✓	✓
Mail.ru	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
myMail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
Email App for Gmail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS

Product	*Command Injection*			*Session Fixation*		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Citadel (929)	●	●	●	◐	●	●
Courier (1.0.14)	✓	●	◐	✓	◐	✓
Exchange (2016)	✓	✓	✓	✓	✓	✓
Gordano GMS[12] (20.06)	✓	●	●	–	–	–
IceWarp (Deep Castle 2)	✓	✓	✓	◐	✓	✓
IPswitch IMail (12.5.8)	◐	✓	✓	◐	●	●
Kerio Connect (9.2.12)	◐	✓	✓	✓	✓	✓
MailEnable (10.30)	✓	✓	✓	◐	✓	✓
MailMarshal[13] (10.0.1.203)	◐	✓	✓	✓	✓	✓
MDaemon (20.0.3)	✓	✓	✓			
SmarterMail (100.0.7503)	✓	●	✓			
Zimbra (8.8.15)	✓	◐	◐			
Exim (4.94#2)	✓	∅	∅			
netqmail (1.06[14])	◐	∅	∅	◐		
Postfix (3.5.4)	◐	∅	∅	✓		
Qmail Toaster (1.4.1)	●	∅	∅	–	∅	∅
Qmail Toaster (1.03-3.3.1)	✓	∅	∅	✓	∅	∅
Sendmail (8.16.1)	✓	∅	∅	–	∅	∅
spamdyke (5.0.1)	◐	∅	∅	✓	∅	∅
s/qmail (4.0.7)	●	∅	∅	✓	∅	∅
Cyrus IMAP (3.2.2)	∅	◐	◐	∅	◐	✓
Dovecot (2.3.10.1)	●	✓	✓	∅	◐	✓
Mercury/32 (4.80.149)	●	●	●	∅	◐	✓

8/23

16/23

– Unknown / Untested
◐ Historic vulnerability (fixed)
∅ Protocol not available
✓ No vulnerability found
◐ No working exploit
● New vulnerability

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓	✓	✓	✓	✓	✓	✓	○$_{U_E}$	✓	✓
LineageOS email (9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓	✓	TLS	○$_{B_R}$	✓	TLS	✓	○$_{U_E}$	TLS	○$_{U_A,U_E}$
OS												
30.23.2.2)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$						✓
ixOS)												
	✓	✓	○$_{C}$[1]	✓	✓	✓						○$_{U_A}$
	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓						○$_{U_A}$
	✓	∅	✓	✓	∅	✓						✓
	●$_{N_S}$[2]	✓	✓	◐$_{B_R}$	◐$_{B_R}$	✓						✓
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]	●$_{N_P}$	✓	✓	◐$_{B_R}$	✓	✓	◐$_{T_M}$	✓	✓	○$_{U_A}$
Trojita (0.7.20190618)	✓	∅	✓	✓	∅	◐$_{B_R}$	✓	∅	◐$_{T_M}$	✓	✓	○$_{U_A}$
Claws (3.17.4)	✓	✓	✓	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	○$_{U_A}$
Sylpheed (3.7.0)	✓	✓	●$_{N_S}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓	○$_{U_A}$
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$	✓	✓	✓	✓	✓	◐$_{T_M,C}$	✓	○$_{U_E}$	○$_{U_A}$
Mutt (1.13.3)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
NeoMutt (20200417)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]	∅	∅	✓	∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook	✓	TLS	✓	✓	TLS	✓	✓	✓	✓	✓	TLS	✓
Yandex.Mail	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	TLS
GMX Mail Collector	∅	●$_{N_S}$	●$_{N_S}$	∅	✓	✓	✓	✓	✓	✓	✓	✓
Mail.ru	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
myMail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS
Email App for Gmail	●$_{N_S}$	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	✓	✓	∅	TLS

16/28

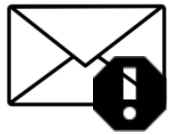
Internet Scanning

Command Injection

Internet Scanning

Standard scanning best practices:

Blocklist



Abuse Mails

Identification

Website

Challenges of Mail Server Scanning

MTAs won't talk to everyone

Email specific Blocklists

SMTP server

DNS Config

- MX
- PTR

Email Specific Allowlists

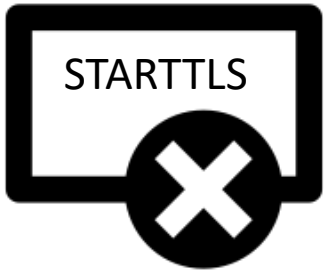
IPv4 Internet Scanning

How many servers are still vulnerable to the command injection (2011)?

Protocol (Port)	Scanned	Vulnerable	Ratio
SMTP (25)	5,521,868	97,697	1.8%
SMTP (587)	4,200,995	58,793	1.4%
SMTP (per IPv4)	7.278,279	111,599	1.5%
POP3 (110)	4,285,730	110,882	2.6%
IMAP (143)	4,165,826	98.773	2.4%
Total	15,729,835	321,254	2.0%

Countermeasures

Mitigation



Disable STARTTLS

Isolate the
Plaintext Phase

Fix Buffering
Issues

Streamline Negotiation

Tales from Disclosure

Client	Negotiation			Buffering			Tampering			UI Spoofing		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Android (Google Play)												
Gmail (8.5.6.199637500)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Gmail Go (8.5.6.197464524)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
Samsung Email (6.1.12.1)	✓	✓	●$_{N_S}$	✓	✓	✓	✓	✓	✓	✓	✓	✓
K-9 Mail (5.710)	✓	✓	✓	✓	✓	✓	✓	✓	✓	○$_{U_E}$	✓	✓
LineageOS email (9)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Apple iOS (App Store)												
iOS Mail (iOS 13.5.1)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	✓	✓
Gmail (6.0.200614)	✓	∅	✓	◐$_{B_R}$	∅	◐$_{B_R}$	✓	✓	✓	✓	∅	✓
Edison Mail (1.20.8)	✓	∅	TLS	◐$_{B_R}$	∅	TLS	✓	✓	TLS	✓	∅	TLS
Windows												
Outlook (16.0.13001.20338)	✓	TLS	✓	✓	TLS	○$_{B_R}$	✓	TLS	✓	○$_{U_E}$	TLS	○$_{U_A,U_E}$
Apple macOS												
Mail (3608.80.23.2.2)	✓	✓										
Linux (tested on NixOS)												
Balsa (2.5.9-1)	✓	✓										
Evolution (3.34.4)	✓	✓										
Geary (3.34.2)	✓	∅										
KMail (19.12.3)	●$_{N_S}$[2]	✓										
Cross-platform (tested on NixOS)												
Thunderbird (68.7.0)	✓	○$_{N_S}$[1]										
Trojita (0.7.20190618)	✓	∅										
Claws (3.17.4)	✓	✓										
Sylpheed (3.7.0)	✓	✓										
Alpine (2.21)	✓	✓	●$_{N_P,N_R}$	✓	✓	✓	✓	✓	◐$_{T_M,C}$	✓	○$_{U_E}$	○$_{U_A}$
Mutt (1.13.3)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
NeoMutt (20200417)	✓	✓	●$_{N_P}$	◐$_{B_R}$	◐$_{B_R}$	◐$_{B_R}$	✓	✓	✓	✓	○$_{U_E}$	✓
OfflineIMAP (7.3.2)	∅	∅	●$_{N_S}$[3]	∅	∅	✓	∅	∅	✓	∅	∅	✓
Cloud Mail (Android & iOS)												
Outlook												
Yandex.Mail												
GMX Mail Collec												
Mail.ru												
myMail												
Email App for Gm												

Product	Command Injection			Session Fixation		
	SMTP	POP3	IMAP	SMTP	POP3	IMAP
Citadel (929)	●	●	●	◐	●	●
Courier (1.0.14)	✓	●	◐	✓	◐	✓
Exchange (2016)	✓	✓	✓	✓	✓	✓
Gordano GMS[12] (20.06)	✓	●	●	–	–	–
IceWarp (Deep Castle 2)	✓	✓	✓	◐	✓	✓
IPswitch IMail (12.5.8)	◐	✓	✓	◐	●	●
Kerio Connect (9.2.12)	◐	✓	✓	✓	✓	✓
MailEnable (10.30)	✓	✓	✓	◐	✓	✓
MailMarshal[13] (10.0.1.203)	◐	✓	✓	✓	✓	✓
MDaemon (20.0.3)	✓	✓	✓	◐	◐	✓
SmarterMail (100.0.7503)	✓	●	✓	✓	✓	✓
Zimbra (8.8.15)	✓	◐	◐	✓	◐	✓
Exim (4.94#2)	✓	∅	∅	✓	∅	∅
				◐	∅	∅
					∅	∅
				–	∅	∅
					∅	∅
					∅	∅
					∅	∅
				∅	◐	✓
				∅	◐	✓
				∅	◐	✓

– Unknown / Untested
◐ Historic vulnerability (fixed)
∅ Protocol not available
✓ No vulnerability found
◐ No working exploit
● New vulnerability

This means a lot of disclosure …

I'd like to report a security vulnerability, but don't know how.

#385 by duesee was closed on 17 Jun 2020

✓ No
○ Mi
◐ Tampering with the mailbox or client state.
● Sensitive data, e.g., emails or credentials, are exposed.
TLS Only implicit TLS configurable.
∅ Not available.

N_R Malicious Redirect
B_R Response Injection
T_M Tampering
U_A IMAP Alerts
U_E Error Messages
C Crash

- Documented behavior

IMAP (143)	4,165,826	98.773	2.4%
Total	15,729,835	321,254	2.0%

Lessons Learned

- No Client was meant to be opportunistic
- Developers were usually aware of the Command Injection in SMTP
  - ➔ But not necessarily in POP3 and IMAP
- Contacting developers/admins is still hard (Add a security.txt please!)

Disclosure of Scan Results

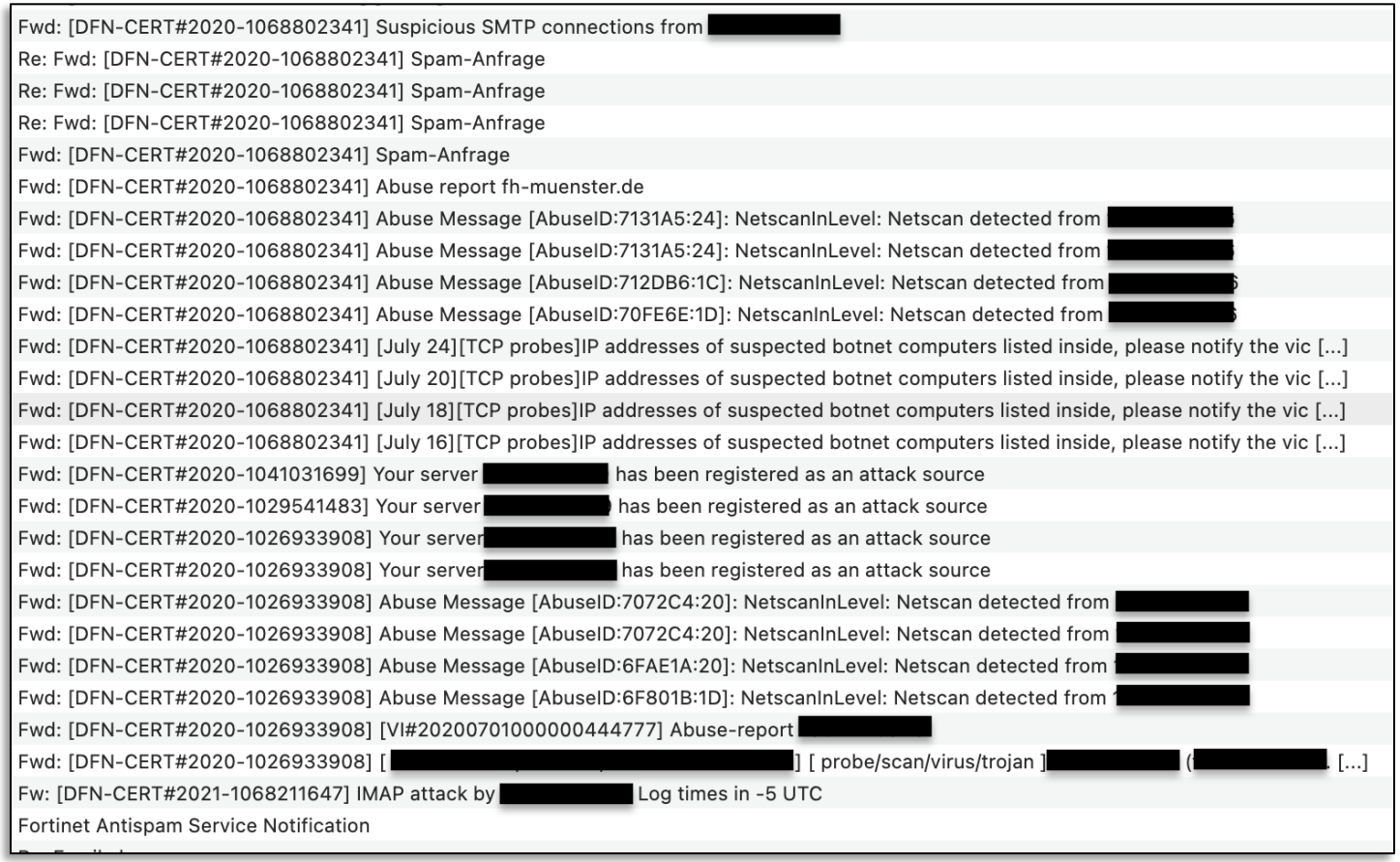
- Communicating scan results to affected admins is hard
- Even if you contact them, what do you tell them?
  - Cannot always tell which server they use from scans
  - Patches are not always available
- Thanks to the BSI CERT
  - Handled communication with server admins in Germany
  - Contacted national certs

Tales from Disclosure (MSPs)

- One paid a bounty but never fixed the issue
- One silently fixed all issues (and stopped answering our emails)
- One argued that STARTTLS is meant to be opportunistic
- Some never respond/have no way to contact them
- …

Tales from Disclosure (Emails)

- You get a lot of “fun” emails:



Updated by Bogisich Gaston about 1 year ago

Damian Poddebniak wrote:

> *As this issue has not been assigned for over 8 months, I wondered if this is recognized as a security issue?*

I am also facing exact same issue. Is your issue resloved? any recommendation how to solve this issue.?

https://www.my[redacted]

Updated by john bond 7 months ago

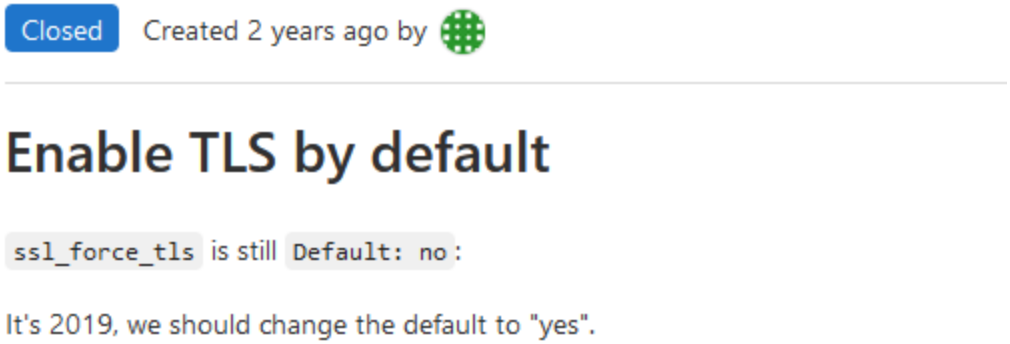
Interestin[redacted]
their webs

https://[redacted]
https://[redacted]
https://[redacted]

Updated by replica watches about 1 month ago

https://www.bestwatcha[redacted]
Sohne-Replica-Watches.ht
https://www.hotwatchs[redacted]
https://www.bestwatcha[redacted]
/Arnold-Son-a-hot.html
https://www.bestwatcha[redacted]
Replica.html https://ww[redacted]
replica.html https://ww[redacted]
https://www.allshopwat[redacted]
https://www.bestwatcha[redacted]

Attack in the wild



Closed Created 2 years ago by

Enable TLS by default

`ssl_force_tls` is still `Default: no`:

It's 2019, we should change the default to "yes".

A previous ticket requested `$ssl_force_tls` to default "yes". I tried that out in release 1.13.0. However, it quickly resulted in a ticket reporting a broken-configuration

In the end is a power-user's MUA with a long history. I decided it was more important to respect existing users and not break their choices and configuration. It's possible I may try re-enabling it again in the future, but probably not for a few more years.

Damian Poddebniak @duesee · 1 year ago

Author

Oh, you mean #135 (closed)?

Looks for me that the user reporting this problem was under an active MitM STARTTLS stripping attempt (Researchers reported Gateways X-ing out STARTTLS.[1])

Edit: I had a look at the trace in #210 (closed) and it really looks like active STARTTLS stripping and not a broken configuration. (Could be from an internal network, but still, someone was meddling with a user connection.) Not sure if the user was aware of that.

```
S: 220 ************************************************************
C: EHLO localhost.localdomain
S: 250-mail.relay.host.name.com Hello localhost.localdomain ([10.10.100.5]), ple
S: 250-XXXA
S: 250-DSN
S: 250-SIZE 163840000
S: 250 PIPELINING
C: STARTTLS
// here, it looks like STARTTLS was replaced by XXXXXXXX
S: 500 Syntax error, command "XXXXXXXX" unrecognized
```

Positive Examples (non-exhaustive)

- Most Open-source developers

- 1&1 Mail & Media GmbH (GMX, Web.de, …)

Open-source Projects

Fixes in RFC9051 – IMAP4Rev2

command (Section 6.2.1). For this reason, the PREAUTH response SHOULD only be returned by servers on connections that are protected by TLS (such as on an Implicit TLS port [RFC8314]) or protected through other means such as IPsec. Clients that require mandatory TLS MUST clo
a non-protec

message. Content of ALERT response codes received on a connection without TLS or SASL security-layer confidentiality SHOULD be ignored by clients. If displayed, such alerts MUST be clearly marked as potentially suspicious. (Note that some existing clients are known
dangerous.) Aler
TLS/SASL confiden

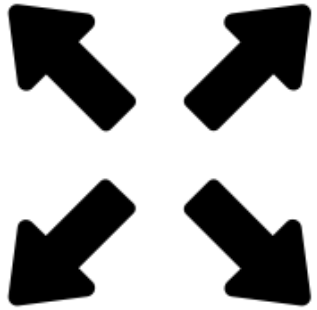
server implementations incorrectly implemented STARTTLS processing and are known to contain STARTTLS plaintext command injection vulnerability [CERT-555316]. In order to avoid this vulnerability, server implementations MUST do one of the following if any data is received in the same TCP buffer after the CRLF that starts the STARTTLS command:

1. Extra data from the TCP buffer is interpreted as the beginning of the TLS handshake. (If the data is in cleartext, this will result in the TLS handshake failing.)

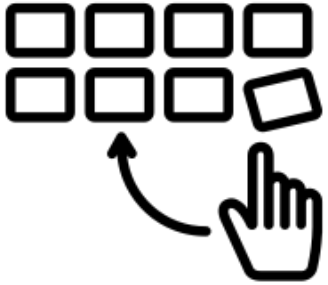
2. Extra data from the TCP buffer is thrown away.

Conclusion

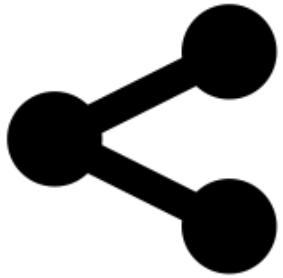
Conclusion



STARTTLS extends the attack surface

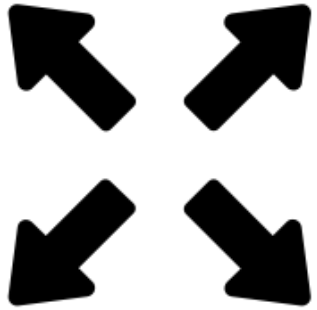


STARTTLS issues are widespread

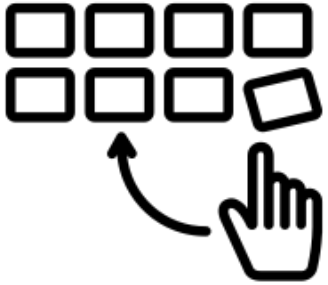


Cross-Protocol Attacks are possible

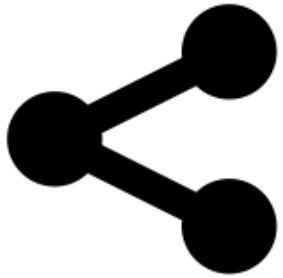
Conclusion



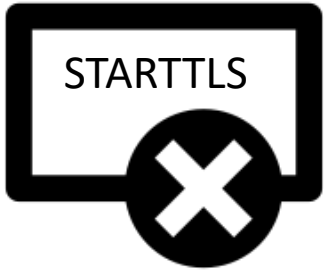
STARTTLS extends the attack surface



STARTTLS issues are widespread



Cross-Protocol Attacks are possible



TLS is better without STARTTLS

E-Mail-Sicherheit im Lernlabor Cybersicherheit (LLCS)

Kurs „Absicherung der E-Mail-Kommunikation”

- Wie laufen moderne Cyberangriffe ab und welche Rolle spielt dabei E-Mail-Sicherheit?
- Ist E-Mail-Sicherheit eigentlich mehr als Phishing-Awareness?
- Was sind SPF, DKIM, DMARC, ... und wie setze ich sie ein?
- Ende-zu-Ende-Verschlüsselung von E-Mails in Unternehmen

https://www.cybersicherheit.fraunhofer.de/sichere-email-kommunikation

http://www.sit4.me/infodienst

Lernlabor Cybersicherheit

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

SLAC 2024

Why TLS is better without STARTTLS:

A Security Analysis of STARTTLS in the Email Context

Fabian Ising[1], Damian Poddebniak[2], Hanno Böck[2], Sebastian Schinzel[1,3]

[1] Fraunhofer SIT | ATHENE Nationales Forschungszentrum für angewandte Cybersicherheit

[2] Independent Researcher

[3] FH Münster

https://nostarttls.secvuln.info/