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

Damian Poddebniak³, Fabian Ising¹,², Hanno Böck³, Sebastian Schinzel¹,²
@dusee@norden.social @murgi@infosec.exchange @hanno@mastodon.social @seecurity@infosec.exchange

¹ Fraunhofer SIT | ATHENE National Research Center for Applied Cybersecurity
² Münster University of Applied Sciences
³ Independent Researcher

https://nostarttls.secvuln.info/
Client-Side E-Mail Ecosystem
Client-Side E-Mail Ecosystem

Network Protocols

- SMTP/Submission
  - RFC 2476, 4409, 5409 (Submission)
  - RFC 5321 (SMTP)
- POP3
  - RFC 1939
- IMAP4
  - RFC 3501 (IMAP4rev1)

Formatting

- IMF
  - RFC 622, 2822, 5322
- MIME
  - RFC 2045-2049
  - RFC 2387

End-to-End Encryption

- S/MIME
  - RFC 1847 (multipart/mixed & multipart/encrypted)
  - RFC 2440 (S/MIME Security)
- OpenPGP
  - RFC 4480 (OpenPGP)
  - RFC 1950 (ZLIB)
  - RFC 1661 (56K SCSI)

Category

- Directly Relevant Standards
- Other Standards

Protocol

- Related Standards
- Other Standards

Relation between Standards

- Uses
- Extends
- Included
Client-Side E-Mail Ecosystem
Client-Side E-Mail Ecosystem

> 150 RFCs
Client-Side E-Mail Ecosystem

> 150 RFCs
> 48 Clients
Client-Side E-Mail Ecosystem

> 150 RFCs
> 48 Clients
> 23 Servers
MSP

Alice (MUA)

smtp.example1.org (MSA)

SUBMISSION (SMTP)

Bob (MUA)

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: IHREDOMAINE\ihrenbenutzername

POSTEINGANGS-SERVER:
- Protokoll: IMAP
- Server: imap.example.org
- Port: 143
- SSL: STARTTLS
- Authentifizierung: Automatisch erkennen
- Benutzername: alice@example.org

POSTAUSGANGS-SERVER:
- Protokoll: SMTP
- Server: smtp.example.org
- Port: 587
- SSL: STARTTLS

Abbrechen  Erneut testen  Fertig
Here be dragons!
Here be dragons!
Introduction to IMAP & STARTTLS
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]

Greeting
IMAP

S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]

C: A CAPABILITY
S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]

C: A CAPABILITY

S: * CAPABILITY IMAP4REV1 AUTH=LOGIN
IMAP

S: * OK [CAPABILITY IMAP4REV1 AUTH=LOGIN]

C: A CAPABILITY

S: * CAPABILITY IMAP4REV1 AUTH=LOGIN

S: A OK
STARTTLS

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

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

// -------------- TLS Handshake --------------
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

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

// -------------- TLS Handshake --------------

C: B CAPABILITY

S: * CAPABILITY IMAP4REV

.. B OK
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

// -------------- TLS Handshake --------------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK
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

// -------------- TLS Handshake --------------
C: B CAPABILITY
S: * CAPABILITY IMAP4REV
.. B OK

Plaintext

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

Damian Poddebnia# 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/poddebnia#k
Questions

Are modern clients opportunistic?
Questions

Are modern clients opportunistic?

What data is sent in plaintext?
Questions

Are modern clients opportunistic?

What is retained from the plaintext phase?

What data is sent in plaintext?
Questions

- Are modern clients opportunistic?
- What is retained from the plaintext phase?
- What data is sent in plaintext?
- What happens in error cases?
EAST Framework

https://github.com/FHMS-ITS/EAST
EAST Framework

https://github.com/FHMS-ITS/EAST
EAST Framework

https://github.com/FHMS-ITS/EAST
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails

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

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S:  * OK [CAPABILITY IMAP4rev1 STARTTLS]
C:  A STARTTLS
S:  A OK NO
C:  B LOGIN "victim" "password"
```
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

S: * PREAUTH
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

S: * PREAUTH
C: A STARTTLS
Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

In addition to the universal commands (CAPABILITY, NOOP, and LOGOUT), the following commands are valid in the not authenticated state: STARTTLS, AUTHENTICATE and LOGIN. See the Security Considerations section for important information about these commands.

C: A STARTTLS
Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

S: * PREAUTH
C: A STARTTLS
```
Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

S: * PREAUTH
C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]

20
Key Findings

• Clients can be tricked into not using STARTTLS
  • Leak credentials or emails

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

15/28 Clients

C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]
Key Findings

- Clients can be tricked into not using STARTTLS
  - Leak credentials or emails
  - Only one library **opportunistic**

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK NO
C: B LOGIN "victim" "password"

S: * PREAUTH
C: A STARTTLS
C: B APPEND Sent {250}
S: +
C: From: victim@example.org
.. Subject: Sensitive Mail [...]
```
Key Findings

• Clients can be tricked into not using STARTTLS

• Many clients process unauthenticated data

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

// -------------- TLS Handshake --------------
Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data

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

// ------------ TLS Handshake -----------
```

![IMAP SERVER ALERT](image)

Your IMAP server wants to alert you to the following:
Please download Microsoft's [https://attacker.com/quickfix.exe](https://attacker.com/quickfix.exe).
More Unauthenticated Data

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

// ---------- TLS Handshake ----------
C: ...
More Unauthenticated Data

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

// ------------
C: ...

[Image of inbox with highlighted "Attacker-Controlled Folder"]
Key Findings

• Clients can be tricked into not using STARTTLS

• Many clients process unauthenticated data

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

11/28 Clients

IMAP SERVER ALERT
alice@example.org
To
This message was sent with High Importance.

Your IMAP server wants to alert you to the following:
Please download Microsoft's https://attacker.com/quickfix.exe.
Key Findings

• Clients can be tricked into not using STARTTLS

• Many clients process unauthenticated data

• Servers vulnerable to known bug

FreeBSD: postfix -- plaintext command injection with SMTP over TLS (CVE-2011-0411)
Command Injection

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

// ----------- TLS Handshake -----------
Command Injection

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

B NOOP

S: A OK

// ---------- TLS Handshake ----------
Command Injection

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

B NOOP

S: A OK

// ----------- TLS Handshake -----------
Command Injection

S: * OK [CAPABILITY IMAP4REV1 STARTTLS]

C: A STARTTLS

.. B NOOP

S: A OK

// ----------- TLS Handshake -----------

S: B OK
Command Injection

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

8/23 Servers
(16/23)
Key Findings

- Clients can be tricked into not using STARTTLS
- Many clients process unauthenticated data
- Servers vulnerable to known bug
  - Many clients vulnerable to a variant

```
S: * OK [CAPABILITY IMAP4REV1 STARTTLS]
C: A STARTTLS
S: A OK
.. B OK
// -------------- TLS Handshake --------------
C: B LOGIN USER PASS
C: C SELECT INBOX
```
Key Findings

• Clients can be tricked into not using STARTTLS
  
• Many clients process unauthenticated data
  
• Servers vulnerable to known bug
  • Many clients vulnerable to a variant

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

16/28 Clients

C: B LOGIN USER PASS
C: C SELECT INBOX
## Impact

<table>
<thead>
<tr>
<th>Attack/Protocol</th>
<th>POP3</th>
<th>IMAP</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Stealing</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Stealing Sent/Drafted Mails</td>
<td>-</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tampering with the Mailbox</td>
<td>X</td>
<td>X</td>
<td>-</td>
</tr>
<tr>
<td>UI Spoofing</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HTTPS Hosting</td>
<td>-</td>
<td>X</td>
<td>-</td>
</tr>
</tbody>
</table>
Mitigation

Enable STARTTLS

Disable STARTTLS
Mitigation

Isolating the Plaintext Phase

STARTTLS
Disable STARTTLS

Isolating the Plaintext Phase
Mitigation

- Fix Buffering Issues
- Disable STARTTLS
- Isolating the Plaintext Phase
Mitigation

- Disable STARTTLS
- Fix Buffering Issues
- Streamline Negotiation
- Isolating the Plaintext Phase
A thank you to the FOSS Developers!

• Response time to bug reports for FOSS Developers was phenomenal!
  • Much better than most commercial vendors ;-}

33
A thank you to the FOSS Developers!

• Response time to bug reports for FOSS Developers was phenomenal!
• Much better than most commercial vendors ;-)

Email-Analysis-Toolkit

Popular repositories

fake-mail-server
Public

command-injection-tester
Public

command-injection-scanner
Public

https://github.com/Email-Analysis-Toolkit
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
Why TLS is better without STARTTLS:
A Security Analysis of STARTTLS in the Email Context

Damian Poddebsniak³, Fabian Ising¹,², Hanno Böck³, Sebastian Schinzel¹,²
@dueseenorden.social @murgiinfosec.exchange @hannomastodon.social @seecurityinfosec.exchange

¹ Fraunhofer SIT | ATHENE National Research Center for Applied Cybersecurity
² Münster University of Applied Sciences
³ Independent Researcher

https://nostarttls.secvuln.info/