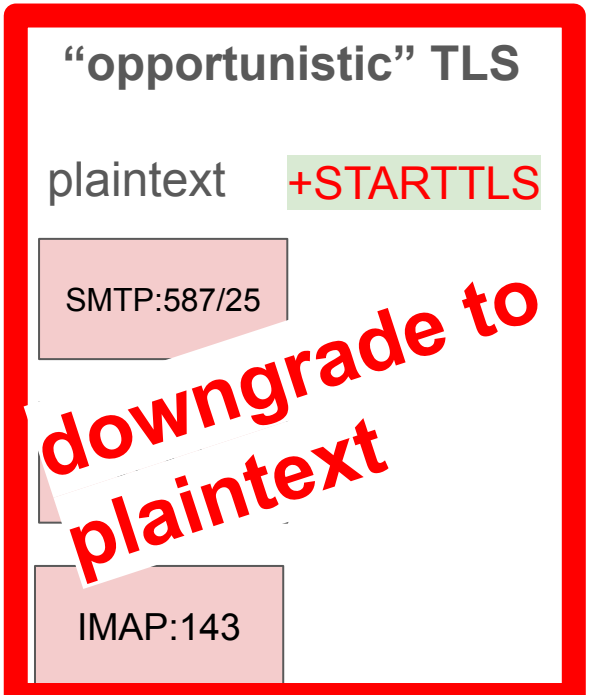
Intermediate Presentation
Email and TLS

Plan

- Protocols and where the vulnerability is
- The downgrade attack + attacker model
- The paper and next steps

Vulnerability



implicit TLS

SMTP:465

POP3:995

IMAP:993

Opportunistic TLS implementation is Client-dependent

O-TLS

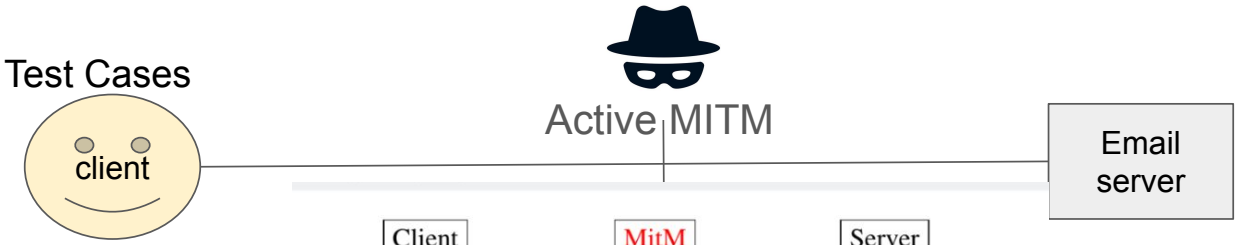
OO-TLS

supports fall back to no-TLS

Is ok

We want to find vulnerable email clients

The attack
4 Security Downgrade Test Cases



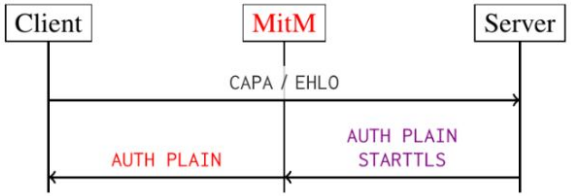


Fig. 2. Classic STARTTLS stripping (test case T_1)

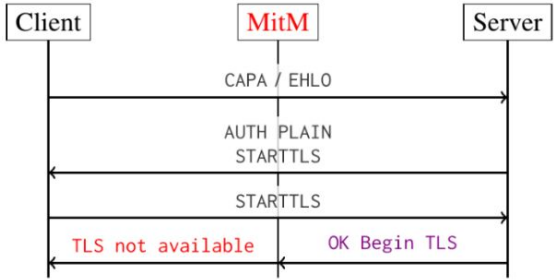


Fig. 4. Return TLS not available in cleartext (test case T_3)

Idea: Make client think that TLS not available

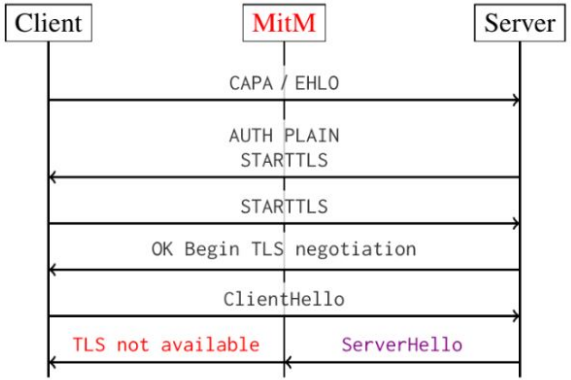


Fig. 3. Replace ServerHello with a plaintext indicating TLS not available (test case T_2)

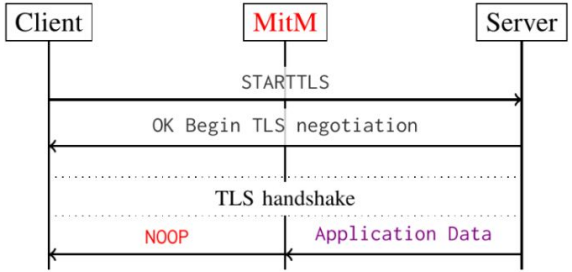


Fig. 5. Disrupt an ongoing TLS handshake (test case T_4)

Possible client-vulnerabilities from findings of the paper

Security Downgrade Test Cases:

- O-TLS versus OO-TLS
- No support for STARTTLS
- Strange implementations of auto-detect of server capabilities

19 out of 49 tested clients downgrade without user notification

Next steps

-> Certificate Validation Test Cases

-> Client behavior when the server advertises plaintext (autoconfig/autodiscovery on server-side) was not in the paper