Communication Networks 2

SS 2019

Assignment 1

Group 08

Name	Mat. Number
Constantin SCHIEBER	01228774
Andreas HIRTENLEHNER	01327273

May 17, 2019

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN
    AUTH=LOGIN] Dovecot ready.
```

Listing 1: Used Protocol IMAPv4rev1, SASL-IR for authentication

```
OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT
    SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MULTIAPPEND
    URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1
    CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY
    MOVE SPECIAL-USE] Logged in
```

Listing 2: IMAP settings

1 Email Password Recovery

1.1 Description of the solution

1.1.1 Used Protocols

Thunderbird uses the protocol IMAP4rev1 (see RFC3501 6.2.2) for the communication with the email server. The framework SASL (Simple Authentication and Security Layer, see RFC442 / RFC 2222) is used for authentification purposes. In the labrotory set-up SASL was configured with the PLAIN flag, which means that all data is exchanged in plain text.

1.1.2 Observed Thunderbird Traffic

We can observe that Thunderbird negotiates its supported capabilities in Listings 1 and 2. Listing 1 shows us that a plain-text authentication process is used, the password should therefore be available in plain-text in one of the following packets.

Listing 3 shows the request for authentication by the server. The client answers with a Base64 encoded string that is shown in listing 4.

```
authenticate PLAIN
```

Listing 3: Request for authentication by server

```
GNuXzA4QGV4MS5jbjJsYWIuY24udHV3aWVuLmFjLmF0AFhpdm9qaWx1cGE4
```

Listing 4: Base64 encoded message

1.1.3 Decoding the message

The message can be decoded with any Base64 decoder tool, the result can be seen in Listing 5. For this exercise, an online tool (`https://www.base64decode.org/`) was used. The client answers to the challenge of the server with its username and password, both transmitted as plain-text.

1.2 Decoded Password

The password can be deducted by removal of the mail address from the Base64 decoded string and is `Xivojilupa8`.

```
cn_08@ex1.cn2lab.cn.tuwien.ac.atXivojilupa8
```

Listing 5: Base64 decoded message

1.3 Strategies to secure the communication

1.3.1 Transmission over TLS

If a plain-text authentication process is obligatory, one can resort to transmission of the plain-text password over a channel that is protected by TLS (Transport Layer Security). This protects from passive eavesdropping, but doesn't prevent man-in-the-middle attacks.

1.3.2 Salted Challenge Response Authentication Mechanism (SCRAM)

Preventing man-in-the-middle attacks presumes that the endpoints assures their identities to each other. Therefore, SCRAM (see RFC5802) in combination with certificates and TLS can be used as an alternative to the PLAIN authentication mechanism. Furthermore, it protects against offline attacks on the password and user database by storing just password hashes.