Lab 14 – MQTT Sikkerhet I

1 Mosquitto directories and files

We will use this directory structure:

- **auth** # to store acl and password files
- **certificates** # to store certificates
- **config** # to store different config files

2 Mosquitto and passwords

2.1 Using the mosquitto_passwd utility

The **mosquitto_passwd** utility is in the **mosquitto** directory.

The Mosquitto information concerning passwords:

- https://mosquitto.org/man/mosquitto_passwd-1.html
- Run **mosquitto_passwd** to get more info

2.2 mosquitto.conf

A complete copy of **mosquitto.conf** is provided (it's from a Windows's install).

Before making any changes to **mosquitto.conf**, make sure that you have a backup copy.
It may be a good idea to have a several different config files available. See 1.4 for how to make mosquitto run the config file you want it to use.

2.2.1 Changes to be made

Look up the "Security" section in the provided **mosquitto.conf** file (it contains useful info):

```
allow_anonymous false

password_file <path/filename>

use_username_as_clientid true
```

Make the changes and save the file (this too will require adm rights) in the **config** directory. Give it a meaningful name.

2.3 Using the mosquitto_passwd utility, part II

Run the password utility to create passwords for the client's "ping" and "pong". You will need adm rights to do this in the mosquitto directory.

```
mosquitto_passwd -c dat235.passwd ping
```

The utility will then ask for a password for ping (and have it confirmed). Next password:

```
mosquitto_passwd -b dat235.passwd pong <password>

mosquitto_passwd -b dat235.passwd pang <password>
```

[Warning: use of -b option: command line history will now store the password[1]]

The passwordfile is a textfile, so you can look it up.

Now, as you probably have realized, the passwordfile should not be visible to anyone but those explicitly authorized to see it.

You take measure yourself here.

Our example uses:

```
ping  Random_01
pong  Random_02
pang  Random_03
```

Store the password file in the **auth** directory.

2.4 Restart mosquitto to take the new settings into account

If you start/stop mosquitto from the command-line, it may be a good idea to specify which config file to use.

```
mosquitto -c config/mosquitto.conf -v
```

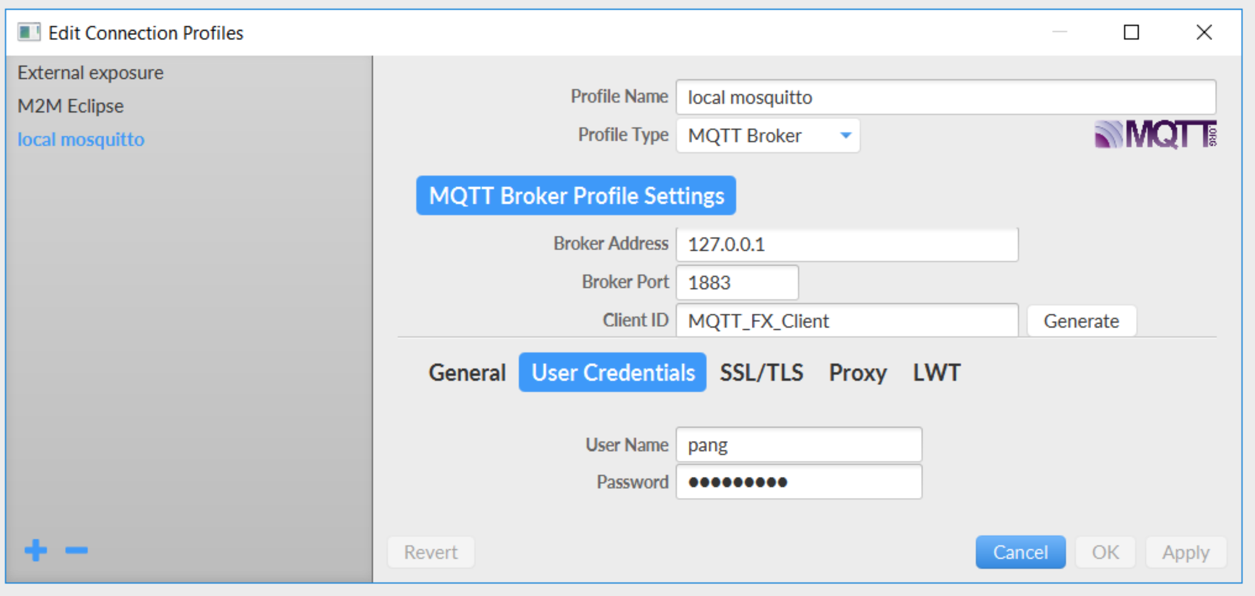
[1] An alternative is to create new password files for each client. Then you join the password files into the one you will actually use (they are textfiles, so this is quite simple).

2.5 Check with MQTT.fx

Try to connect with MQTT.fx. You should get the “Not authorized to connect” error.

Then:

Edit your connection profile & try again. Here we have **pang**. The password must of course match.



Edit Connection Profiles

External exposure
M2M Eclipse
local mosquitto

Profile Name: local mosquitto
Profile Type: MQTT Broker

MQTT Broker Profile Settings

Broker Address: 127.0.0.1
Broker Port: 1883
Client ID: MQTT_FX_Client

User Name: pang
Password: ●●●●●●●●●

Then you run the **Ping.py** and **Pong.py** programs (at the same time, use different command boxes).

Check out the code.

3 Access control

Access control is by means of an access control list. The attached **dat235.acl** is an example.

3.1 The ACL file

The acl file is a textfile. See “access control” in https://mosquitto.org/man/mosquitto-conf-5.html

Check out the attached acl file (which matches the **ping**, **pong**, **pang** users).

Store the acl file in the **auth** directory.

3.2 Enabling use of an access control list

Open the (whatever name) **mosquitto.conf** file and find the **acl_file** entry.

```
acl_file auth/dat235.acl
```

Save the file and restart the broker.

Verify that ping and pong can publish/subscribe as before, and that pang only can subscribe.

If you run the broker from the command line, then try this:

```
mosquitto -c config/mosquitto.conf -v
```

The broker will log when it denies access to a topic.

```
1539858185: Denied PUBLISH from pang (d0, q0, r0, m0, 'dat235/pingpong', ... (2 bytes))
```

4 Final words

These files are sensitive files:

- mosquitto.conf
- the password list
- the acl list

That means that they should have protection and not be accessible to every user on the system.