

TNE20003 – Internet and Cybersecurity for Engineering Applications

Portfolio Task – Project

Aims:

To integrate all of the knowledge you have acquired in this unit into a solution to an identified problem in your field of engineering/science. Solve the problem and securely transfer the data.

Preparation:

- All of your lectures & labs

Due Date:

- This task is to be completed by the beginning of week 12. It is to be presented during either your lab session or tutorial session. We will post a list of presentation times which will allocate to you the day and time of your presentation. Once your presentation is completed you must upload all documents up to Canvas to ensure that you complete and hand the task in on time.

Background

You consulting company has been hired to develop a new Engineering Solution for a Client. This solution must contain the ability to function within an online, Internet of Things Environment. Your manager has assigned you the task of developing the prototype solution for the Internet component of the Project.

The Client has advised that they have already deployed a IoT infrastructure for existing projects, and would like this solution to leverage this installation. Your design must use the existing IoT infrastructure to broker communications between components.

IoT Infrastructure

The Client is running the MQTT (Mosquitto) Message Broker on: **rule28.i4t.swin.edu.au**

In order to allow your product to utilise this infrastructure, an account has been created for this project. The username for this account is your student ID (if your ID contains an 'x', then it uses a lowercase 'x'). The password for this account is equal to the username, ie. Your student ID.

The MQTT Protocol defines a message broker service, clients are authorised and connect to the server, following which they may post messages to a variety of topics AND subscribe to topics. When subscribed to a topic, the client will receive all messages posted to that topic. Topics are hierarchical, for example, a message posted to the topic (site/entrance/temperature) is posted to the top-level topic site, 2nd level topic entrance, and bottom level topic temperature. MQTT supports an infinite topic depth.

As the MQTT infrastructure is shared by multiple projects, your account has restrictions as to what topics you can post or subscribe to:

- You can only post/subscribe to the top-level topic <username> where <username> is the username you logged into the server with. You are free to create as many sub-topics as you like under this top-level topic.
- All projects can post/subscribe to the top-level topic `public`. You are free to create as many sub-topics as you like under this top-level topic.

When posting messages to MQTT, you must specify the exact topic that the message gets posted to.

When subscribing to a topic, you may subscribe to wildcard topics. There are two wildcard characters:

- + – Subscribe to any sub-topic at this level
- # – Subscribe to all sub-topics at this level and all deeper levels

For example:

- `site/+/temperature` – Subscribe to all `temperature` topics at the site for all locations (not just entrance)
- `site/#` – Subscribe all all sub-topics of the `site`

Experimentation with IoT Infrastructure

You are encouraged to download a graphical MQTT Client from [Graphical Client](#). Note that clients are available for Windows, Mac and Linux. You can use this client to connect to the MQTT Server, post messages, and subscribe to topics. Note that if you subscribe to the public topic, you will receive messages posted by all students.

You should also experiment with subscribing to wildcard topics to understand how the MQTT subscription process functions.

Requirements

You are to nominate a reasonable application within your chosen Engineering Major (Biomed/Electrical/Robotics/Software) or your chosen IT Major. Within this application, you need to devise at least two end devices, of which at least one must be responsible for both posting and receiving messages from the broker. For example, I have a final year project group who are implementing a solution to aged care issues. They are developing a “Personal Anomaly Detector” to determine when an aged person has had a significant event take place like a health emergency or mistreatment from staff. They are using the MQTT system for the message of this data from device on the aged person’s body to the central nurse station.

As highlighted by the EMQX website: [mqtt with python](#)

[MQTT](#) is a lightweight messaging protocol for IoT in [publish/subscribe model](#), offering reliable real-time communication with minimal code and bandwidth. It is especially beneficial for devices with limited resources and low-bandwidth networks, making it widely adopted in IoT, mobile internet, IoV, and power industries.

Python is widely used in IoT for its versatility, ease of use and vast libraries. It's ideal for smart home automation, environmental monitoring and industrial control due to its ability to handle large amounts of data. Python is also compatible with microcontrollers, making it a valuable tool for developing IoT devices.

You will be required to implement the devices as Python applications (to eventually be incorporated into the real solution). Your applications should create fake data at intervals to post to the MQTT broker, and receive and parse requests to perform an action (eg. Turn light on) from the broker. Requests to perform an action should be printed to screen.

You are required to build a Python application to act as a user interface to the final solution, monitoring system state and issuing commands/updates to the system.

You are required to prepare a report on the Cybersecurity issues around the existing MQTT broker deployed by the Client.

Assessment

Pass

- Implement one client device which generates data and posts messages to a private topic on the MQTT server.
- Implement one client device which subscribes to an appropriate topic and prints received messages to the screen. Client should also subscribe to the public channel and print all public messages along with their sub-topic information.
- Use a graphical MQTT client to demonstrate received messages from device 1.
- Use a graphical MQTT client to demonstrate generating a message and sending it to device 2.
- Provide source code for applications and instructions on how to run it.

Credit

All Pass tasks above PLUS:

- One of the device applications must both generate messages AND subscribe to a topic.
- Both device applications must subscribe to the public topic.
- The Client MQTT broker runs within the organisation providing a site-wide IoT solution. Access is blocked from off-site. Provide a Cybersecurity report detailing the security issues with the current deployment of the MQTT broker.

Distinction

All Credit tasks above PLUS:

- At least two devices must subscribe to different topics, responding to different requests/posts.
- At least one device must generate messages to more than one topic.
- Replace the Graphical MQTT client with a Python Client to act as a simple user-interface to monitor the system and generate/post messages.

High Distinction

All Distinction tasks above PLUS:

- The monitoring application must generate commands to send to the devices (via the MQTT broker) based on messages received from the devices (eg. If temperature exceeds value then issue command to enable fan cooling).
- The Client wishes to open their IoT infrastructure over the Internet to enable usage at other sites. Extend your Cybersecurity report to consider issues faced with the current deployment by making access to the MQTT broker over the Internet.
- This will attain a basic HD result. To attain any bonus marks, you must use your imagination and add extra functionality.