University of Glasgow | School of Computing Science

# Assessed Coursework

| | | | | |
|---|---|---|---|---|
| Course Name | Networked Systems (H) | | | |
| Coursework Number | Exercise 1 | | | |
| Deadline | Time: | 3:00pm | Date: | 10 February 2022 |
| % Contribution to final course mark | 10% | | | |
| Solo or Group ✓ | Solo | ✓ | Group | |
| Anticipated Hours | 10 | | | |
| Submission Instructions | Submit via Moodle | | | |
| Please Note: This Coursework cannot be Re-Assessed | | | | |

## Code of Assessment Rules for Coursework Submission

Deadlines for the submission of coursework which is to be formally assessed will be published in course documentation, and work which is submitted later than the deadline will be subject to penalty as set out below.

The primary grade and secondary band awarded for coursework which is submitted after the published deadline will be calculated as follows:

(i) in respect of work submitted not more than five working days after the deadline
  a. the work will be assessed in the usual way;
  b. the primary grade and secondary band so determined will then be reduced by two secondary bands for each working day (or part of a working day) the work was submitted late.

(ii) work submitted more than five working days after the deadline will be awarded Grade H.

Penalties for late submission of coursework will not be imposed if good cause is established for the late submission. You should submit documents supporting good cause via MyCampus.

**Penalty for non-adherence to Submission Instructions is 2 bands**

**You must complete an "Own Work" form via https://studentltc.dcs.gla.ac.uk/ for all coursework**

# Networked Systems (H) 2021-2022 – Exercise 1

Dr Colin Perkins, School of Computing Science, University of Glasgow

27 January 2022

## Introduction

The third laboratory exercise reviewed secure communication and protocol ossification. It asked you to consider some of the principles of secure communication, the operation of Transport Layer Security (TLS), and the QUIC transport protocol. This exercise builds on that work, to further test your understanding of those protocols and your ability to apply that understanding. **This is an assessed exercise that is worth 10% of the marks for this course.**

## Assessed Exercise 1

This assessed exercise comprises four questions. You should prepare and submit a written report that answers all four of these questions.

**Question 1:** The Transport Layer Security (TLS) protocol uses a combination of symmetric and public-key cryptography. Explain why this is done, and how it ensures both security and good performance. [5 marks]

**Question 2:** When used with TCP, TLS operates within a TCP connection. The connection begins with an initial three-way handshake to establish a TCP connection, which is followed by the TLS v1.3 handshake running within that connection to negotiate security parameters, and only then is data sent. In contrast, when used with QUIC, the TLS v1.3 handshake messages are sent in the same packets as the messages performing the QUIC connection establishment handshake. Explain why the QUIC transport protocol combines these two sets of messages into the same packets. Discuss whether it would be possible to similarly extend or modify TCP to include the TLS v1.3 handshake messages along with the packets that perform the initial TCP handshake. Consider and discuss what would be the challenges and (potential) benefits of doing so. [10 marks]

**Question 3:** The nature of secure communication protocols, such as TLS, is that they protect data in transit between endpoints but not the data stored within the endpoints. For example, a messaging application might use TLS to protect messages while they are being sent between users and the messaging server, while not protecting the messages while they are being processed within the messaging server. Facebook Messenger is an example of such a service. Discuss whether you think such a service provides meaningful security and/or privacy. Describe, with examples, the threats such a service protects against, and those against which it offers no protection. [10 marks]

**Question 4:** Discuss how you might modify a messaging system, such as that described in Question 3, to prevent the server from accessing messages while they are being processed, outlining the key challenges in making such a change. [5 marks]

## Submission

You should submit a single report, in PDF format, answering the four questions given above. A mark out of 30 will be assigned to your submission, weighted as noted earlier. This mark will be converted to a percentage, then used to assign a band on the University's 22 point scale.

Prepare your PDF file formatted for A4 paper, in two columns, using the Times Roman font in 10pt, with 1.5cm margins (i.e., using a format that matches this page of the handout). If you use LaTeX to prepare your document, the following structure will format your submission appropriately:

```
\documentclass[10pt,a4paper,twocolumn]{article}
\usepackage[cm]{fullpage}
\usepackage{newtxtext}
\usepackage{newtxmath}
\begin{document}
\title{Networked Systems (H) Exercise 1}
\author{matriculation number goes here}
\date{date goes here}
\maketitle
...answers go here...
\end{document}
```

You are not required to use LaTeXwhen preparing your report. Your report must not exceed two pages in length, including all figures, tables, and any references. *Length is not an indication of merit.* If you can answer the questions in less than two pages, then please do so.

You must submit your report before 3:00pm on 10 February 2022. Following the code of assessment, late submissions will be accepted for up to 5 working days beyond this due date. Late submissions will receive a two band penalty for each working day, or part thereof, the submission is late. Submissions that are received more than five working days after the due date will be awarded a band of H.

Submissions must be made via Moodle. This problem set is worth 10% of the mark for this course. Submit a single PDF file entitled `ns-ex1-GUID.pdf`, replacing *GUID* with your GUID (your student number followed by the first letter of your surname). Submissions that do not follow these submission instructions will be given a two band penalty. Penalties will be strictly enforced.

If you are ill, or have other circumstances that may affect your submission, then you may contact the course coordinator *before* the deadline to request an extension, following the usual procedure.