University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	**Networked Systems (H)**			
Coursework Number	**Exercise 1**			
Deadline	**Time:**	**4:00pm**	**Date:**	**23 February 2023**
% Contribution to final course mark	**20%**			
Solo or Group ✓	**Solo**	✓	**Group**	
Anticipated Hours	**20**			
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) 2022-2023 – Exercise 1

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

9 February 2023

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 20% of the marks for this course.**

Assessed Exercise 1

Prepare and submit a report that answers the following 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 initial three-way handshake establishes the TCP connection, then the TLS v1.3 handshake running within that connection negotiates security parameters, and only then is data sent. In contrast, when used with QUIC, the TLS v1.3 handshake messages are sent along with the packets that complete the QUIC connection establishment handshake. First, explain why the QUIC transport protocol combines these two sets of messages into one exchange. Then, discuss whether you think the benefits of overlapping the connection establishment and security handshake outweigh the cost of changing the protocol. Your answer should include examples, with justification, of scenarios where the change is beneficial and scenarios where it is not. [20 marks]

Question 3: Discuss whether it is possible to somehow extend, or modify, TCP to include the TLS v1.3 handshake messages along with the TCP packets that perform the connection establishment handshake. Explain what would be the challenges and (potential) benefits of doing so. Describe the different options for encoding the TLS handshake into TCP to support this behaviour, giving specific details of the changes to TCP and TLS that might be required, and outlining the strengths and weaknesses of the different approaches. Discuss whether the resulting protocol would be deployable and usable in practise. [25 marks]

Question 4: Another feature provided by the QUIC transport protocol is the ability to send multiple streams of data within a single connection. One of the claimed benefits of this feature is that it helps to prevent *head of line blocking* between streams. Explain what is head of line blocking and how it is caused, discuss why it might be problematic, and outline how the use of multiple streams in QUIC avoids those problems. [10 marks]

Submission

You should submit a single report, in PDF format, answering the four questions given above. A mark out of 60 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, and with the exercise title, your GUID (matriculation number and initial letter of your surname), and the date at the top of the first page (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{GUID goes here}
\date{date goes here}
\maketitle
\section*{Question 1}
...answers go here...
\end{document}
```

You are not required to use LaTeXwhen preparing your report. Your report must not exceed three 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 three pages, then please do so.

You must submit your report before 4:00pm UK time on 23 February 2023. 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 20% of the mark for this course. You must 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 are formatted incorrectly, that have the wrong filename, or that otherwise 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.