University of Glasgow | School of Computing Science

Assessed Coursework

Course Name	**Networked Systems (H)**			
Coursework Number	**Summative exercise 1**			
Deadline	**Time:**	**4:30pm**	**Date:**	**13 February 2020**
% 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) 2019-2020 – Exercise 1

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

30 January 2020

Introduction

The lecture in week three of the Networked Systems (H) course has considered secure communication, and the Transport Layer Security (TLS) protocol. **This is a summative exercise worth 10% of the marks for this course** that aims to explore your understanding of TLS.

Summative Exercise

There are three parts to this exercise. You should prepare and print a single report that includes your answers to all three parts.

1. TLS uses hybrid encryption to ensure communication is both efficient and secure. The initial handshake uses a public key scheme (the ephemeral elliptic curve Diffie-Hellman key exchange algorithm) to negotiate keys, then the ongoing communication uses either AES or ChaCha symmetric encryption. Explain, in your own words, why the combination of both public-key and symmetric encryption is needed to ensure communication is both secure and has high performance. **[5 marks]**

2. Version 1.3 of the TLS protocol was completed in August 2018. It is a significant update from the previous version, TLS v1.2, that dates from a decade earlier. TLS v1.3 corrects a number of problems, improves performance, and offers a number of new features. For part two of your report, read about what has changed between TLS v1.2 and v1.3 and, in your own words, write a summary of what you think are the key improvements, fixes, and changes in the newer version of TLS. The following may be useful:

   - `https://tools.ietf.org/html/rfc8446`
   - `https://ietf.org/blog/tls13/`
   - `https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/`

   but you can, and should, read other documents and blog posts as needed. Be sure to cite all your sources, and if you include direct quotes from other material be sure they are clearly marked. **[20 marks]**

3. One of the changes in TLS v1.3 was the addition of 0-RTT connection establishment when a client is connecting to a server with which it has previously communicated. The benefit of 0-RTT connections is faster performance; the risk is that 0-RTT data is subject to replay attacks. Explain what is a replay attack and describe how can you safely use 0-RTT data with TLS v1.3. **[5 marks]**

Submission

You should submit a single printed report covering the topics outlined above. A mark out of 30 will be assigned to each 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.

There is no single correct answer for this exercise. Marks will be assigned for technical correctness, for well-researched arguments that have reasoned justification, and for presenting clear, coherent, and well-structured arguments. The goal is to test your ability to conduct research, read and summarise technical documents, to clearly state opinions on the suitability of new technologies, and to write an executive summary of the results. It is likely, and expected, that different answers will highlight different features of the protocol, especially in part two of the report. You should state your opinions, with technical justification based on your background reading. It is noted that different people may legitimately have different opinions on the importance of various features, and that the marking will support this.

Format your report for A4 paper, formatted 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 preamble will format your submission appropriately:

```
\documentclass[10pt,a4paper,twocolumn]{article}
\usepackage[cm]{fullpage}
\usepackage{newtxtext}
\usepackage{newtxmath}
\begin{document}
...
```

You are not required to use LaTeX. Your report must not exceed two pages in length. Length is not an indication of merit; if you can answer the question in less than two pages, please do so.

You must submit your report before 4:30pm on 13 February 2020. Your submission should comprise a single PDF file entitled `netsys-ex1-`*`GUID`*`.pdf`, replacing *`GUID`* with your GUID (your student number followed by the first letter of your surname). Submissions must be made via Moodle. Submissions that do not follow these submission instructions will be given a two band penalty. Penalties will be strictly enforced.

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.

This problem set is worth 10% of the mark for this course. You are reminded that this means it should take approximately ten hours to complete, likely split approximately evenly between reading and writing. There is a lot of information available about TLS, and it is possible to spend much longer than ten hours on this report. The intent is *not* that you write the most comprehensive report possible, but rather that you write the best report you can *within ten hours*.