The University of Melbourne
School of Computing and Information Systems
COMP90043 Cryptography and Security

Research Project, Semester 2 2020

Due Date: 31 October 2020 - 23:59 AEDT

1 Introduction

The project will be carried out in groups of maximum three students. If someone prefers to work alone or cannot find a group, we can allow individual projects. However, we encourage everyone to work in a group.

Your topic can be chosen from the list of potential research topics in the Appendix. Some suggested reading has been provided in the references section for your convenience. Other topics may also be suitable. Please consult your tutors if you wish to select an alternative topic.

The university library[1] provides free access to a wide range of scholarly publications. You are encouraged to search for recent journal and conference articles on the listed topics. You can also use the textbook and the lectures as a starting point. Otherwise, you may also want to search for scholarly material via Google Scholar.

The term paper project contributes 35% of your total mark in the subject. The project involves two parts; the first part is a recorded presentation and the second part is a written report. Part 1 (the presentation) is worth 10% of your total mark and Part 2 (the written report) is worth 25% of your total mark for the subject.

2 Research Report

2.1 Part 0: Project Proposal

Each group will first need to decide a topic that you wish to work on, and write a brief proposal. A project proposal should include at a minimum a background section with cited references, team members and an introduction / motivation section. The proposal should not exceed two pages.

2.2 Part 1: Presentation of Video Recording

Each group will prepare a video recording of 8-10 minutes with companion presentation slides on their topic during Week 10 of Semester 2 2020 (the week starting Monday 12th October 2020). Details of exact presentation time during that week will appear later. Students should gain a reasonable understanding of the topic and be able to answer questions from their classmates after playing the video recording. An electronic version of the video recording must be accessible publicly. A URL to fetch the media content must be submitted at the designated submission area on LMS (details appear later) by 06:00 AEDT Monday 12th October 2020.

2.3 Part 2: Written Report

Students must also submit a written report on the topic. The size of the report depends on the number of students in the group.

- Individual projects: 2400 words
- Group of Two: 2800 words
- Group of Three: 3200 words

Word count excludes references and diagrams. The written report should be in the form of a research paper. You are encouraged to author your reports and presentations in `LaTeX`, though it's not a must. If you have selected a topic from the literature track, the work is expected to present some insight that is not publicly accessible with ease. Otherwise, if you have selected a topic from the experiment track, the report should present insightful evaluations as to what has been investigated in the experiment. The work should be scholarly.

You should acknowledge any suitable reference you utilized to prepare the term paper. You are also required to include a conclusion section about your evaluation and critique of the topic. The originality of thought in the analysis and narration will receive a higher weightage while marking using the marking criteria mentioned below. The report is due by 23:59 AEDT - Saturday 31st October 2020 and should be uploaded to the `Assignments > Research Project` section of the COMP90043 LMS. Only the group leader should submit the report and (optionally) project artifacts. Submission of project artifacts is not necessarily for groups on the literature track

[1] https://library.unimelb.edu.au/

and optional for groups on the experimental track. Late submission will be possible but will attract late penalties, unless under special circumstances.

Note: It is not necessary to complete the written report at the time of the presentation. However, you need to present the main aims of your research, the general methodology adopted for the work, and the planned references for the report. You can continue to improve the report after the presentation using the feedback from the teaching team as well as from your group's self-reflection.

3 Timeline for Research Report Project

No.	Activities	Due Dates
1	Group Registration	September 6, 2020 (23:59 AEST)
2	Project Proposal Submission	September 13, 2020 (23:59 AEST)
3	Submission of recorded presentation	October 12, 2020 (6:00 AEDT)
4	Submission of written research report	October 31, 2020 (23:59 AEDT)

4 Marking Criteria

Part 1: Presentation (10 marks)	
Coverage of the Major Themes within the Topic	40%
Clarity of Presentation	20%
Presentation of Technical Details	20%
Use of Accessible Examples	10%
Critical evaluation	10%

Part 2: Written Report (25 marks)	
Format and Structure	10%
Quality of Sources Cited	20%
Coverage of the Topic	20%
Critical evaluation	30%
Presentation of the Technical Details	20%

4.1 Mark Allocation in Groups

All members of a group will get the same mark on the project, and all members must contribute to both the presentation and the written report. If a member does not contribute to a part of the project, then that member will get no marks allocated for that particular part. The first page of the report should have a short reflective statement by each member explaining his/her contribution (about half a page per person). The project proposal should outline the expected contribution of each group member. If you have any concerns about the contribution of group members not being equal, please discuss this with the teaching team.

5 Administration

5.1 Getting Help

If you have any questions, the LMS discussion board will be a useful resource in resolving any issues. If your concern is a personal matter, then you should email the subject coordinator.

Any answers posted by the subject coordinator on the LMS discussion board will be considered as part of the project specification. In addition, please keep an eye out for any LMS announcements for any changes made to the project specification.

5.2 Academic Honesty

Turnitin will be used as a deterrent against academic dishonesty. The report should consist of your original work. All citations should be made in an academically recognised style, which should be used consistently throughout the report. Direct quotes should be minimal, and should be clearly highlighted by the use of quotation marks and also cited properly. If you reproduce any diagrams, they should be clearly acknowledged.

Plagiarism and collusion constitutes cheating. Disciplinary action will be taken against students who engage in plagiarism and collusion in accordance with university statute 13.1.18. For examples and more information on what constitutes plagiarism and collusion, please visit http://academichonesty.unimelb.edu.au.

5.3 Grievances

In the event that your group arrangements does not work out as planned or some member(s) in your group has not contributed at all, you should raise this immediately with the head tutor Lianglu (lianglu.pan@unimelb.edu.au). It is imperative that you understand that not much can be done when the grievances are raised towards the project deadline.

5.4 Group Registration

The group registration is available on the LMS. It's under **People** section and then **Groups**.
If you failed to register yourself into a group, you may be placed into an empty group and will work on your own. You may register for a group once you have all your group membership confirmed. We will lock the group registration after the registration due date, but you can freely switch between groups before that.

5.5 Report Submission

The deadline for the final report submission is as specified at the start of this project document.

The report must be submitted as a PDF file on the LMS. A cover sheet which includes names of all group members should be included in the first page. The report is to be formatted on A4 sized paper in 10 pt text, with 1.5 line spacing and a minimum 3.8 cm margins on the left and right sides. The content you write should be present in the PDF file in the form of **text**, rather than as screenshots and/or images of the text you wrote.

Links and exact submission instructions will be posted to the LMS.

5.6 Errata

Any updates to this specification sheet will be recorded here - if necessary.

A Literature Track

Cryptography

Stream Cipher

Block Cipher

Cryptographic Commitment Schemes

Database Encryption

Digital Signature Schemes

Cryptographic Game Theory

Zero-knowledge Proofs

Post-Quantum Cryptography

Security

Security in Mobile Applications

Efficient Key Management Schemes

Security in Operating Systems

Security in IoT

Privacy through Cryptography

Email Encryption

Secure End-to-end Messaging Protocols (i.e. Signal Protocol)

Privacy-Preserving Frequent Itemset Query over Encrypted Database

Other topics are welcome, so as long as they fall under one of the 3 domain headings.

B Experimental Track

Fast Prime Factorisation

Digital Signature Scheme Evaluation

Cipher Suite Evaluation

Proof-of-* Implementations

Simulated Security Exploits (Network, Systems)