Monash University FIT5163,

SEMESTER 2, 2020

Mini Research Report (25%)

Group Assignment

Due Date: Sunday 08 November 2020 (11:55pm)

- This is a group assignment. **Form a group of 3 students within your tutorial slot ONLY. (2 students per group is only allowed for leftover.)**
- You will present this work as a group in your **Week 12 Tutorial Slot.**
- **NO MARK WILL BE GIVEN TO THE WHOLE ASSIGNMENT** if you have not come to the presentation (without any acceptable reason, e.g. a medical certificate), even if you have submitted your report or your groupmate has presented the result. **Therefore, you cannot pass the hurdle and will fail the unit!!!**
- **FULL MARK: 25 MARKS (Report: 18 Marks. Presentation: 7 Marks)**

Overview

This assignment is a **mini research project**. You will select a specific area in cyber security, and each group need to **read at least 3 technical papers (for the group of 3 students) or at least 2 papers (for the group of 2 students)** about your selected area. Then you will **discuss and maybe analyse these papers** based on their approaches, contributions, methods, limitations, and any other criteria.

You will submit your presentation materials and the group report together **in a ZIP file. Each group only needs to submit one ZIP file, by any one of the group member.**

You will do research on one of the cyber security areas to gain a better understanding of the state-of-the-art in this field. You will write your findings in a high quality report **(no more than 6 pages and no less that 5 pages, 11pt font, single column, normal margin, default line spacing)**. This part must demonstrate your ability to study and discuss peer-reviewed journal articles or conference papers, carry out in-depth analysis, and arrive at substantial conclusions. You will also present your findings in your Week 12 Tutorial slot (maximum 15 minutes for each group including Q&A).

Step 1 - You need to select only one of the following topics:

- Cryptology
- Applied cryptography
- Lightweight security
- Database security
- Implementation Issues on Cryptography

- Blockchain or Cryptocurrency

Step 2 - After selecting your research area, you need to read and research the related journal articles or conference papers **published on or after 2010** from the following list:

Journal Article: • IEEE Transactions on Information Forensics and Security • IEEE Transactions on Dependable and Secure Computing • Journal of Cryptology
Conference Paper: • Crypto • Eurocrypt • Asiacrypt • Australasian Conference on Information Security and Privacy (ACISP) • Applied Cryptography & Network Security (ACNS) • Theory of Cryptography Conference (TCC) • International Conference on Practice and Theory of Public-Key Cryptography (PKC) • RSA Conference Cryptographers' Track (CT-RSA) • Financial Cryptography and Data Security (FC) • European Symposium on Research in Computer Security (ESORICS) • ACM Conference on Computer and Communications Security (CCS) • ACM Asia Conference on Computer & Communications Security (ASIACCS) • USENIX Security Symposium (USENIX Security) • Network and Distributed System Security Symposium (NDSS) • IEEE Symposium on Security and Privacy (IEEE S&P) • IACR Cryptographic Hardware and Embedded Systems (CHES)

- **If you do not use papers from the above conference/journal list without the approval of your tutor, then the assignment will get a zero mark**

- You may find your selected papers from the **online databases** in Monash Library: IEEE, ScienceDirect, Springer, ACM, ProQuest, IOS Press, or Scopus.

- You will select *at least* **2 related papers** (if your group contains 2 members) or **3 related papers** (if your group contains 3 members). There should be a clear connection between the topic, analysis and the findings that the papers of each group are discussing/proposing. **If the papers are not related in topic and discussed work, the assignment will get 50% reduction on its total marking.**

After identifying the papers that you want to work with you must show them/discuss them with your tutor BEFORE starting to work on them so that he/she can provide you feedback on their suitability for the assignment. Only then you can consider them selected. You must finalize the papers that you are using at most 2 weeks before the deadline of the assignment

Step 3 - After selecting your papers, you need to identify each paper's contributions, the proposed approach/method, the research issues/challenges it addresses, main findings and finally any remaining open issues. You need to read, understand and analyse each paper and provide a professional and brief description for each:

- The **research challenges and issues** that each paper addressing (there might be more than one paper addressing the same issue)
- **The paper contributions,** what **approach/method/model** they are proposing and developing to address those challenges**.** You need to briefly describe their proposed approaches/methods/models, *avoiding technical details and jargons.*
- What are **the main findings and results** of each paper (usually discussed after the evaluation section), and **any open issues** for further research, if any.

Step 4 – You will consolidate all the results of step 3 into **one single research report (per group)** following the specified guidelines below.

You need to follow the following structure:

1. **Papers Publication Details:** titles, authors, publication venue (journal name, journal volume number, page number, year; conference name, page number, year) **(0.5 mark)**

2. **Introduction:** a brief description on what your papers are about. **(2 marks).**

3. **Brief Summary:**
   a) Discuss the **challenges/issues** that these papers focus on; **(3 marks)**
   b) Briefly and clearly describe **the technical contribution** of each paper (that is, how the paper has outperformed the other schemes in the past, in terms of functions; and/or security; and/or efficiency etc.); **(3 marks)**
   c) Summarize the **approach of the new findings and results of evaluation/experiments**. **(4 marks)**
   d) Add **your judgement** on their results at the end. (e.g. If the papers address the same problem, here you need to **compare how their improvements are different** or which approach outperforms the other one.) **(3 marks)**

   To write this section, **use paragraphs** rather than bullets or other styles, and make sure the paragraphs have a logical and consistent flow.

4. **Conclusion** - Conclude by saying what the papers were about, briefly discussing the main or interesting findings and making your final point. **(2 marks)**

5. **References** (this will not be counted in the page limit) **–** list the details of all the references you used in preparation of the report**. (0.5 mark)**

Step 5 – You will present your findings in your Week 12 tutorial slot. You can have maximum 15 minutes (including Q&A) per group to present your finding. **Each group only needs to make one presentation**. **Each student needs to present their corresponding part. (7 marks)**

Submission Requirements:

All the following files should be uploaded to Moodle as a zip file and use the following naming convention: FIT5163-A2-[StudentID1-StudentID2-StudentID3].zip (assume there are 3 students in this group). **Only one group member needs to upload** the file. **There is a mark deduction for any missing document**.

1. An Assessment Cover Sheet for the group
2. The presentation material (in pdf format)
3. The report (in pdf format)
   Note: Hand-written report is NOT accepted. No mark will be given to any hand-written report.

Late Submission:

Late Assignments or extensions will not be accepted unless you submit a special consideration form and provide valid documentation such as a medical certificate prior to the submission deadline (NOT after). Otherwise, there will be **10% penalty per day including weekends.**

PLEASE NOTE.

Before submitting your assignment, please make sure that you haven't breached the University plagiarism and cheating policy. It is the student's responsibility to make themselves familiar with the contents of these documents.

Please also note the following from the Plagiarism Procedures of Monash, available at http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-procedures.html