**Group Assignment**

 This is a group assignment. **Form a group of 2 or 3 students within your tutorial slot**

**ONLY.**

 You will present this work as a group **.**

 **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, 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 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

 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)

 You may find your selected papers from the **online databases**  in 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).

**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) Summarise 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 paper was 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:**

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.