Singapore Polytechnic
School of Computing

ASSIGNMENT TWO

INTRODUCTION

This assignment constitutes (20%) of your in-course assessment as mentioned in the module overview.

OBJECTIVE

The learning objectives of this assignment is to reinforce the cryptographic concepts and information security principles covered in the module.

The students will be tasked to:

- Validate familiarity with security concepts.
- Reinforce use of cryptography in business situations.
- Analyze the pitfalls of the existing applications.
- Propose countermeasures.
- Select the preferred countermeasures and implement the solution.

These tasks are aimed at studying the proper information security controls in the process and technology aspects.

INSTRUCTIONS

1. Students are to complete the assignment in group.
2. Submit your **implementation** (Code package) on **Week 17**, 10th Feb 2023 (Fri) 2359 via Polymall
3. Arrange your group interview/demo session on **Week 18** with your tutor (13th Feb – 17th Feb 2023).
4. Late submission will incur penalty in marks.
5. Read the following sections of this document for task details and report requirements.

TASK DETAILS

Your team has developed an automated menu system (So Power Automated Menu 2 – SPAM2) with a whole list of features.

With overwhelming demand and limited budget, the management has decided to setup additional outlets outside SP, using public WIFI (e.g. Wireless@SG).

The sample source code given is for your evaluation and reference. You can modify them based on your team's design and implementation. Please note that **the sample programs contain no security features**.

Your group is tasked to enhance the design, and implementation to provide the needed security with other enhancement features.

Please note that it has been decided by the management that the **menu-of-the-day** information required only **integrity** protection in transit. However, the **day-closing** information required both **confidentiality** and **non-repudiation protection**.

Your team has been tasked to:

- Conduct a security risk assessment. (See appendix A)
- Create a proposal to overcome the security risks identified. (See appendix B)
- Implement the solution (See appendix C)
- Arrange a demonstration session with your tutor on week18 (13^{th} – 17^{th} Feb 2023)

In summary, your group should propose and implement security mechanisms needed to **ensure the confidentiality, integrity,** and **non-repudiation** of important data being exchanged and stored.

ASSESSMENT CRITERIA

The assessments of this assignment will be based on following:

1. Proposal Report (60%)
   - Report clarity, formatting, technical content, risk assessment.

2. Application – server Program (15%), client Program (15%)
   - Technical functionalities of programs – suitable use of cryptographic algorithm
   - Robustness, completeness and usability of the programs
   - The level of challenges

3. Key Management (10%)
   - Creation and use of Public Key Infrastructure, or
   - Protection of keys and important data, or
   - Implementation of protocol to support the required functionalities.

Note: You are allowed to use 3^{rd} party Python modules to implement your solution.

Warning: Plagiarism means passing off as one's own the ideas, works, writings, etc., which belong to another person. In accordance with this definition, you are committing plagiarism if you copy the work of another person and turning it in as your own, even if you would have the permission of that person.
Plagiarism is a serious offence, and if you are found to have committed, aided, and/or abetted the offence of plagiarism, disciplinary action will be taken against you. If you are guilty of plagiarism, you may fail all modules in the semester, or even be liable for expulsion.

Appendix A

Risk assessment is an integral part of project management, information security, and software development.

In this assignment, we will only perform risk assessment for **confidentiality**, **integrity,** and **non-repudiation** of the data stored and exchanged, with consideration on the deployment of the software.

In your risk assessment, you should consider the following steps:

1. Identify the processes that should be protected.
2. Identify threats associated with **confidentiality**, **integrity** and, **non- repudiation**.
    - Storage (data at rest)
    - Communication channel (data in transit)
3. For each of the threats, specify the security goal(s) that is/are affected.
4. Suggest possible countermeasures/controls for each of the threats identified.
    - The suggested countermeasures/controls should be feasible.
    - The team must be able to implement the proposed solution in your final software product.

Complete the simplified risk assessment form (Simplified_Risk_Assessment_Form.doc) and attached it as an appendix of your **proposal**.

	SEVERITY			
	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW – 1 –	MEDIUM – 4 –	MEDIUM – 6 –	HIGH – 10 –
POSSIBLE RISK WILL LIKELY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 11 –
PROBABLE RISK WILL OCCUR	MEDIUM – 3 –	HIGH – 7 –	HIGH – 9 –	EXTREME – 12 –

*Use the risk matrix above to complete the **severity** and **likelihood** columns in the form.*

Additional information on software risk assessment:
https://www.synopsys.com/blogs/software-security/software-risk-analysis/

Appendix B

PROPOSAL REQUIREMENTS

1. The proposal should be about 10 pages, excluding appendices (single-line spacing, 12-point fonts).
2. Proper report structure should include cover page, content page, introduction /background, others and appendixes.
3. Cover page of your proposal should include:
    - Module name (Applied Cryptographic) and code (IT8084).
    - Course and class.
    - Name of students
4. Outline of the proposal
    - Illustrate the current SPAM2 system and its implementation (e.g. connected via Wireless@SG)
    - Describe any additional **assumptions** made on the implementation.
    - Describe the various attack scenarios, propose countermeasures with justification.
        - Make reasonable assumptions on the motivation and capability of attackers.
        - Make reasonable assumptions on the potential impact.
    - Illustrate the proposed system
        - Highlight the new features added their roles in data protection.
5. Conclusion & additional considerations
6. Planned task allocation
7. Individual reflection
8. References
    - If you use any materials in your report, please quote the reference.
    - You can refer to books, journals, or online resources, please remember to acknowledge the source.
9. Appendix – Completed risk assessment form

Appendix C

1. Each member should indicate his/her contributions using comments in the python code.
2. List the work done by each member in the **contributions.txt** file**.**

SUBMISSION CHECKLIST

Compress your project in a zip file (code package) with the following structure and upload to Blackboard.

\ (Base directory)
+ readme.txt – Briefly explain how to run the program
+ contributions.txt - List the work completed by each member
+ source files - Python files (with sub-directories)
+ deployment files - Additional files needed such as certificates, private / public keys and etc