Singapore Polytechnic
School of Digital Media and Infocomm Technology

ASSIGNMENT TWO

INTRODUCTION

This assignment constitutes part of your in-course assessment (30%) as mentioned in the module overview. It is important that you allocate sufficient time to complete this assignment.

OBJECTIVE

The learning objective 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.
- Analyse the pitfalls of the existing applications.
- Propose countermeasures.
- Select the preferred countermeasure 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 groups of 3-4 members.
2. Report and source codes (both soft copy) are to be submitted into the assignment dropbox on Blackboard by **Week 18 Wednesday 11.00 PM**.
3. Late submission will incur penalty in marks.
4. Read the following sections of this document for task details and report requirements.

TASK DETAILS

The chat server enables secure communication within 2 or more parties over a network, such as over a Local Area Network (LAN) or over the Internet. One of the computers acts as a chat server, and the other acts as a chat client.

Mr Larochelle has implemented 2 sets of simple Client, Server programs (both and text based or GUI based) to illustrate the implementation chat protocol (http://www.dreamincode.net/forums/topic/259777-a-simple-chat-program-with-clientserver-gui-optional/). The basic programs are for illustration and contain no security features.

Your group is tasked to improve the basic chat programs by Mr Larochelle. You need to be aware that not all of the chat application users are benign, and identify the possible attacks to the current implementation. Your main objective is to improve on

the security features of the chat programs. A secondary goal is to enhance the implementation of the chat functionalities based on the given code.

Your group has been tasked to:

- Conduct a security risk assessment on the provided chat programs
- Propose a suitable solution
- Implement the solution
- Produce a report on your finding and implementation of solution

REPORT REQUIREMENTS

1. The report should be about 15 pages, excluding source codes and appendices (single-line spacing, 12-point fonts). The team should ensure that all the important points are covered.

2. Proper report structure should include cover page, content page, explanations of your work, learning reflections, and task allocation.

3. Cover page of your report should include:
   - Module name and code.
   - Course and class.
   - Name of students (sort by student admission no, in ascending order).

4. Documentation of work includes the
   - Write-up on the analysis of security risk assessment and the proposed countermeasures with justification.
   - This is a project that encompasses all of the material taught in class. Students are expected to apply what they have learned both in-class and off-class to solve application problems.

5. Security risk assessment and implementation
   - You should analyse the application flow carefully and try to identify the pitfalls or risks found in the software prototype.
   - You are encouraged to make reasonable assumptions on the motivation and capability of attackers.
   - In your risk assessment, you should consider the following steps:
     a) Identify the process that should be protected.
     b) Identify all possible threats and vulnerabilities.
        i. The client-side program.
        ii. The server-side program.
        iii. The use of cryptographic functions to mitigate the risks.
        iv. The usability of programs. These include ease of use, user interface, error trapping, etc.
        v. Communication channel between the applications.
     c) For each of the threats, specify the security goal(s) that is/are affected.
     d) Suggest possible countermeasures/controls for each of the threats identified. The suggested countermeasures/controls should be

feasible and the team must be able to implement the proposed solution in your final software product.

6. References
   - If you use any materials in your report, please quote the reference.
   - You can refer to books, journals, or online resources. But please remember to acknowledge the source.

TOOLS

Use Java JCE (Java Cryptographic Extension) to implement your solutions. Basic cryptographic primitives such as key agreement, signature, encryption, decryption, public-key infrastructure (PKI) has been covered in practical exercises.

ASSESSMENT CRITERIA

The assessments of the assignment will be as follows:

1. Written Report (30%)
   - Report Clarity – marks are awarded for those who present their reports neatly and completely.
   - Report Technical Contents – marks are given according to the quality of the work done.
   - Report Format – marks are given according to the layout and format of the work done.

2. Application – Server Program (25%)
   - Technical Functionalities of programs – use of cryptographic algorithm
   - Authentication and authorization
   - Robustness and Completeness of programs
   - The level of challenges

3. Application – Client Program (25%)
   - Technical Functionalities of programs – use of cryptographic algorithm
   - Authentication and authorization
   - Robustness and Completeness of programs
   - The level of challenges

4. Application – Identity Management (20%)
   - Creation and use of Infrastructure or protocol to ensure integrity and non-repudiation of the messages sent.
   - The level of challenges

5. Bonus (Maximum 15%)
   - Additional functionalities (e.g. private messaging to ensure confidentiality).
   - Refinement in the graphical user interface

SUBMISSION CHECKLIST

1. Softcopy of:
   - Report (WinWord format).
   - Source codes (Java source files).

Warning: plagiarism – any group found plagiarising in this assignment would be penalised. Marks awarded for the report will be equally divided for the parties involved.