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 in softcopy) are to be submitted in Blackboard by **Week 18 Wednesday (15th Aug 2018) 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 File Transfer Protocol (FTP) enables transferring files between two computers over a network, such as over a Local Area Network (LAN) or over the Internet. One of the computers acts as an FTP server, and the other acts as an FTP client.

Your group has been assigned as Application Security Consultants for IHL (Institute of Higher Learning) Technology Pte Ltd, a software house that develops customised computer software applications.

IHL has recently completed a client-server software prototype. The software is a simple client-server file transfer application, with little or no security features built into the application.

Your group is tasked to secure the basic FTP programs.

As application security consultants, you need to understand the business needs of the company, the purpose of the applications and what are needed to improve the programs. The main objective is to improve the **security features** within the programs, and also to implement secure communication channel between the client and the server.

Your team has been tasked by the Chairman of IHL to:

- Conduct a security risk assessment on the software prototype
- Propose a suitable solution to overcome security risks identified in the risk assessment
- Implement the solution
- Produce a report on your finding and implementation of solution

The source codes for both the client Client.java and server Server.java prototype programs will be uploaded to the Black Board.

You group should propose and implement security mechanisms needed to **ensure the confidentiality, integrity and non-repudiation** of the message being exchanged.

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. Therefore, it is **very important** to make sure that you understand all ACG practical sessions.

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
   - Robustness, completeness and usability of the programs
   - The level of challenges

3. Application – Client Program (25%)
   - Technical Functionalities of programs – use of cryptographic algorithm
   - Robustness, completeness and usability of the programs
   - The level of challenges

4. Application – Key Management (15%)
   - Creation and use of Public Key Infrastructure, or
   - Protection of Symmetric Keys, or
   - Design and implementation of protocol to support the required functionalities.
   - The level of challenges

5. Bonus (Maximum 5%)
   - Refinement in the graphical user interface

Note: You are allowed to use open-source libraries in C to implement your solution.

SUBMISSION CHECKLIST

Softcopy of:

- Report (Word format).
- Codes
  - Java source files (it could be either be (1) only the source folder or (2) the complete IDE project folder)
  - Deployment files. Ensure that you program is deployable by instructions given in deployment files.
    1. Run program by using standard java –jar option
       - i.e. *java –jar acg_server.jar* or *java –jar acg_client.jar*.
       - You are strongly recommended to test the deployment files in the lab PCs before submission.
    2. Readme.txt – Very important. Please clearly explain how to run the program. **Marks will be deducted if program is not able to run during marking**

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.