COMP3334 Computer Systems Security

Group Project (25%)

[Deadline: 23:59:00 5th Dec 2016 (Mon)]

Form yourselves a group of 3 – 5 students. Please create a group and ask your group members to enroll on blackboard (using the Groups Tab on the left) by 1st Nov. You may also make use of this function to recruit group members.

Background

In this project, you are going to implement a software solution pertaining to computer and information security. The project aims to strengthen your concepts in computer security, in terms of cryptography, authentication, access control and web security, by applying these concepts to the development of a practical application that satisfies desirable security properties.

What you have to do

Examine ONE of the following applications. Propose and implement a (desktop/mobile/Web-based) software solution with desired security properties:

1. **Instant Messaging**

   Instant messaging allows text-based real-time communication among individuals. These days, people are concerned about the privacy of their messages during transmission public networks. Also, integrity and authenticity of the origin of messages have to be guaranteed when the application is used in an untrusted environment.

2. **E-Voting System**

An e-voting system allows voters to cast a ballot over a network. The ballot should be kept secret and intact during transmission and storage. Voters' should remain anonymous to the public about their cast. Accountability should be ensured that only the absolutely necessary entities should have access to the voting system and its data.

3. Password Manager

A password manager allows its user to keep his/her password in an encrypted vault. It either allows you to keep the encrypted vault locally, or to sync it across all your devices. To enforce a strict access control for the vault, two-factor authentication could be employed.

4. Cloud Storage System

A cloud storage service allows its user to outsource their data to the cloud. A secure cloud storage system should protect the confidentiality of the outsourced files. More advanced system would even protect the confidentiality against the cloud server. How data integrity could be ensured is another concern that should be addressed.

Write a report. It should contain the following sections:

a. Problem statement
b. Security requirement analysis
c. Design specification
d. Application setup guide
e. Conclusion of your contribution
f. Bibliography

Only major compulsory sections are listed above. You may include sub-sections so that your report is presented in a more systematic manner.

Your report must NOT exceed 30 pages, excluding the cover page, the table of contents and appendices of supplementary documents (e.g., diagrams, figures, and screenshots), with single line spacing and font size 12. Use .doc/.docx/.pdf format for the report only. Use the APA or IEEE standard to format all citations.

Assessment Criteria

The assignment is assessed based on the following criteria:

Requirement Analysis (5%)	Identify security issues based on previously gained knowledge and/or literature review or comparison with existing systems. Also include other functional/non-functional system requirements.
Identification of Appropriate Tools / Mechanisms (5%)	Identify the appropriate tools and mechanisms to address the security requirements. Show an understanding of the underlying assumptions.
System Design and Development (15%)	Design and develop a prototype that satisfies the system requirements.

Submission

The submission deadline of this project is 23:59:00 Mon 5th Dec 2016. No late submission is allowed.

Only the **GROUP LEADER** submits the followings:

- a zip file for both the program and report to Blackboard (if the file is to large, burn it to CD/DVD);
- one HARDCOPY of the report.

The method of submission of the hard copy will be announced in due course.

This is a group project. Each group member must fill in the peer evaluation form. Each student has to rank the contribution of his/her group members, including himself/herself. Submit it individually to our TA. The aim of peer evaluation is to serve as a free-rider deterrent. In case of apparent inconsistency of ratings among group members, a special interview session may be arranged for the group. Students who fail to submit this form are subject to mark deduction.

Plagiarism is a serious offence. Both copier and copiee will be given ZERO mark in this assignment and may be subject to disciplinary action (e.g., academic disqualification).

Peer Evaluation Form

Name:

Student No:

Group Members (Name)	**Effectiveness***				
	Not at all	**Poorly**	**Adequately**	**Well**	**Extremely Well**
<Me>					

* Put ✓ in appropriate boxes