Guidelines for Term Project

Due Dates

December 29 (Tuesday), 2015:	Proposal
January 18–21, 2016:	Demonstration
January 21 (Thursday), 2016:	Final Report

Note: please schedule (about one week in advance) a date and time for demo with the corresponding instructor of your project.

Project Options

Select one from the following four projects:

1. Evaluating the Strength of AES (Yih-Kuen Tsay)
2. Secure Authorization & Patch Download: Applications of Public-Key Cryptography and Hash Functions (Yeong-Sung Lin)
3. Comparing the Speeds of HMAC and CMAC (Yih-Kuen Tsay)
4. OWASP WebGoat – Web Application Security Lessons (Yeali S. Sun)

A detailed description of each project may be obtained from the corresponding instructor or the course website. The description may override some of the guidelines listed below.

General Guidelines

- Find a classmate to form a group of two; you may choose (but are not encouraged) to do the project alone. Email Yih-Kuen Tsay (`tsay@im.ntu.edu.tw`) the project selection of your group as soon as possible. The student groups will be evenly distributed on a first-come-first-serve basis to the four projects. You will be asked to submit another selection when necessary. To save the time of email exchange, you may send your order of preference right in the beginning.
- Any written submission (proposal or final report) should be dropped by the deadline in the mailbox of the corresponding instructor of your project. Late submissions will be penalized. Please use A4 paper and staple in the upper left corner. NO plastic or cardboard covers; NO binders, either.
- The proposal, the demonstration, and the final report all will be taken into account for the grade of your project.
- DO NOT plagiarize (i.e., do not use material without crediting the source).

Proposal

- Give an outline of your design, which should include at least the following:
  - Diagrams showing the overall system architecture
  - How the system components interact and how the user interacts with the system
  - What cryptographic algorithms will be used and why they are chosen
- The proposal should be about 6–8 pages long with reasonable font size and spacing.

Demonstration

- The demonstration should be about 15 minutes long.
- Schedule well in advance a date and time with the corresponding instructor of your project.

Report

- Give a detailed account of the design and implementation of your system; include a brief user guide if possible.
- Your final report should be about 12–16 pages long with reasonable font size and spacing, excluding source code.