CS472: Computer and Network Security
Fall 2010

Implementation Course Project
Due: November 29, 2010

Note: A project team may consist of up to 3 students.

This project combines the concepts of an application-level firewall and a secure application. (i) You are asked to design and implement a secure application (SSTORE) that can offer the following services to students and faculty of an academic institution. It should be a stand alone system in the sense that we should be able to implement it on any legacy systems, and still operate effectively. In that sense, it is self sufficient in terms of the data that it stores. (ii) Implement an independent software-based application gateway APPGATE through which all requests to SSTRORE must be directed. In other words, any requests to SSTORE is ALWAYS routed through the gateway.

SSTORE and GATEWAY are two independent programs. No one access SSTORE directly. All calls to SSTORE must be first filtered by GATEWAY and then forwarded to SSTORE.

The objective of the GATEWAY are as follows:
(i) It only allows requests from specified IP address domains (e.g., only ODU). All other requests are refused immeditealy. (ii) For valid domain users, it authenticates users and allows only authenticated users to have access to the SSTORE. (iii) It receives all requests, parses the commands and make sure that only valid commands are passed to SSTORE. (iv) It logs the user names, the time, and the commands that they have executed. (v) Communication between GATEWAY and SSTORE is via secure channel that is encrypted. So the two ends (GATEWAY and SSTORE) authenticate each other prior to establishing a channel.

The system may be implemented using either Microsoft .Net (on Windows), Java, or any other platform/language.

Your design and implemementation will be evaluated based on the following criteria:
- User interface
- Flexibility: Ability to add/delete users, courses, students, and documents.
- Flexibility to change passwords
- Transparency offered to the users: There should be minimal input from the user due to security features (Don't expect the user to remember hundreds of passwords or encryption keys)
- Forgotten passwords? If a user forgets his/her password, they should not completely lose their documents.
- An administrator should not be able to decrypt the documents.
- Should assume that communication is not secure

Using the system, a faculty member will be able to create courses, add students to courses, add/delete documents, make the documents available to the chosen courses, chosen individuals (students/faculty), and make changes to the earlier given accesses.

A student may be registered in more than one class. Only a faculty member will be able to add/delete a student from his/her class. The system needs to assure the faculty member that all mechanisms are in place to secure the documents.

Your design choices should clearly indicate how they satisfy the above requirements. You should clearly have a demonstratable code that runs. You should submit (i) Code (ii) Report. Place both these on a CD prior to submission.