bSecure – Computerized building security system

Introduction to Software Engineering
Department of Computer Science
Technion – Israel Institute of Technology

Winter 2009-2010

1. General Instructions

1.1 Project Goal
The goal of the semester project is to illustrate the work in a software development group, which applies the methods acquired during the course. The phases in the project include most of the phases in the lifecycle of a software system, the scope of the project, however, matches the time frame of one academic semester.

1.2 The Phases of the Project
The project is executed in groups of four students each. There are four main submissions in the project: requirements phase (10%), analysis phase (25%), design phase (30%), implementation and verification phase (35%). In the first two phases the whole system is defined and analyzed; in latter phases only a part of a system is designed and implemented. The tasks in each phase should be distributed uniformly among the members of the group. Each submission should include a description of the responsibility of each member in executing the relevant phase. One of the members of the team should be assigned as a project manager, who among other duties coordinates meetings, distributes tasks and supervises the process of accomplishing the objectives of each phase. The project employs object-oriented methodologies, using the UML language for the analysis and design phase and the Java language in the implementation phase.

1.3 Grades
Each phase has a different weight in the project's grade (which is 50% of the final grade). Each student in each group receives an individual grade by his/her responsibilities and contribution to accomplishing the objectives of the relevant phase.

Good luck!
2. Requirements Phase
The goal of this task is to simulate the requirements analysis process done with the client. You are required to build the requirements data base, based on the requirements description (in Section 3) and the FAQ section that will be elaborated next.

2.1 Client story FAQ section (Possible 5 points bonus)
While building the requirements data base, some questions may arise. Provided your questions are not clearly answered in the client story itself (section 3), you should send the question, via email, to Roy Levin (royl@cs.technion.ac.il) and cc Pavel Gurevich (pg@cs.technion.ac.il) who will both simulate the client for our purposes. When sending a question, please provide the following information; Student names, ids and emails, and team name. A subset of selected questions will appear in the Client story FAQ document that will be published on 3.11.2009.
Note that some of the answers to the questions in this document will become mandatory requirements, those will be marked accordingly in the document. A team may be granted a bonus of up to 5 points (for the requirements analysis part) provided that they were the first to ask a question which the client finds as being of high significance.

2.2 Requirements Document
Submission Due Date 15.11.2009 at 12:00 noon
The front page should include the following details:
- A unique group name (you may include your logo as well)
- Names and ids of the group members
- Number of cell to return the submission
The submission should also include a short summary of the distribution of the responsibilities among the group members. For the requirements analysis phase of the project you are not obliged to distribute the responsibilities. The requirements analysis and categorization must be done according to Volere, as done in the tutorial. Please use the Volere requirements template from the assignment page.
You should submit a printed paper version to the course mailbox (floor 1) and also submit a pdf version via the course website. To produce pdf documents you may use pdf995 which is a free tool that allows you to print a document to a pdf file.
3. bSecure – Client's Story

bSecure is a fully computerized building security system, comprising a large number of secure sectors, with different security levels. Each security sector is equipped with a camera, powerful speakers, an entrance or exit request button respectively and automatic rotating doors (capable of containing one person) deployed at its entrance and exit points.

Whenever a person arrives at an entrance to a security sector he may express his desire to enter the sector by pressing the request entrance button. The button then turns on and the request is then sent to the central computer which then responds by sending a recorded message to the entrance speakers directing the person to face the camera and wait for the recognition process to end. The camera begins recording and sends the images to another machine which is in charge of recognizing the face and retrieving the person’s unique identification number, hereafter the person's id. The face recognition software is a commercial off-the-shelf product. The central computer then accesses the database to retrieve the person's security restrictions. If the person is allowed access he is instructed, via the speakers, to enter the door and the request entrance button turns off. Similarly, when a person requests to exit a security level he reaches the exit doors, presses the request exit button, the button then turns on, he faces the camera and if no problems are detected he is allowed to exit. When a person exits a security sector the system verifies via its database that in fact the person is listed as having entered this security sector. The information regarding the individual's stay in the sector is recorded by the system.

There are four levels of restrictions. Each restriction level allows access to all security sectors below or equal to it. In other words, personnel with security restriction 3 may access sectors of level 1, 2, or 3 but cannot access sectors of security level 4. A person requesting to enter a security sector with a higher level of security than that which he has can only do so for a limited time, provided he is accompanied by a person with a proper security level.

Security restriction levels are assigned by a system administrator. The administrator has a console which allows him to enter new people into the system and assign security restrictions (levels 1-4) to them. The administrator can access the system by entering his username and password. After the administrator logs on, a welcome
screen is displayed with the administrator's options presented. The administrator may add a new user, change an existing user's security restrictions, or delete a user from the system. When deleting a user, the administrator may also select to add this user to the black list. When entering a person into the black list, the administrator must also provide a reason for doing so in a special comment field. Personnel that are black listed can not be entered into the system again in the future.

A person's details consist of his full name, address, id number, image and a list containing the security restrictions he has been granted since he was registered to the system. The list also contains the starting and ending dates each of these security restrictions have been granted and if revoked, a reason field also exists.

Once a month, the system produces a report containing detailed information about access to each security sector. The report contains the list of people that have entered the areas, the time they spent in each area, and who accompanied them (if relevant).

Whenever a security violation occurs, the administrator is notified and until he responds, no personnel are allowed to enter or exit any security sector (a situation called “lockdown”). The system also announces through the loudspeakers that the building is undergoing a security lockdown due to a breach in security. The administrator is the only one that can turn off the security lockdown and return the system to its standard state.