CS 435 Homework 2 February 17, 2014

Due date: **Feb 24, 2014**

To deliver: **email your solution to**
**Md Atiqur Rahman <mrahman@email.wm.edu>**
**filename: <yourname>_hw2_cs435.pdf**
**fileformat: pdf**

This is **NOT a team effort**, you are expected to do this on your own!
For tools to draw UML diagrams, check the class wiki.

The sequence diagram below describes the authentication for accessing a facebook user account. The diagram is taken from http://www.uml-diagrams.org/ which is a good source of information on UML diagrams!

**Task 1:** Write a fully dressed use case following Larman Ch 6 that matches with the sequence diagram.

For Larman Ch 6, see
http://www.craiglarman.com/wiki/downloads/applying_uml/larman-ch6-applying-evolutionary-use-cases.pdf

**Task 2**: Draw a use case diagram for the use case that results from Task 1.

**Task 3**: Develop classes and a class diagram for each of the involved entities browser, application, authorization server and content server. Start with a single class per entity (= per diagram) and refine it such that you have at least 3-4 nodes per diagram. This will require some creativity on your end. Make plausible decisions.

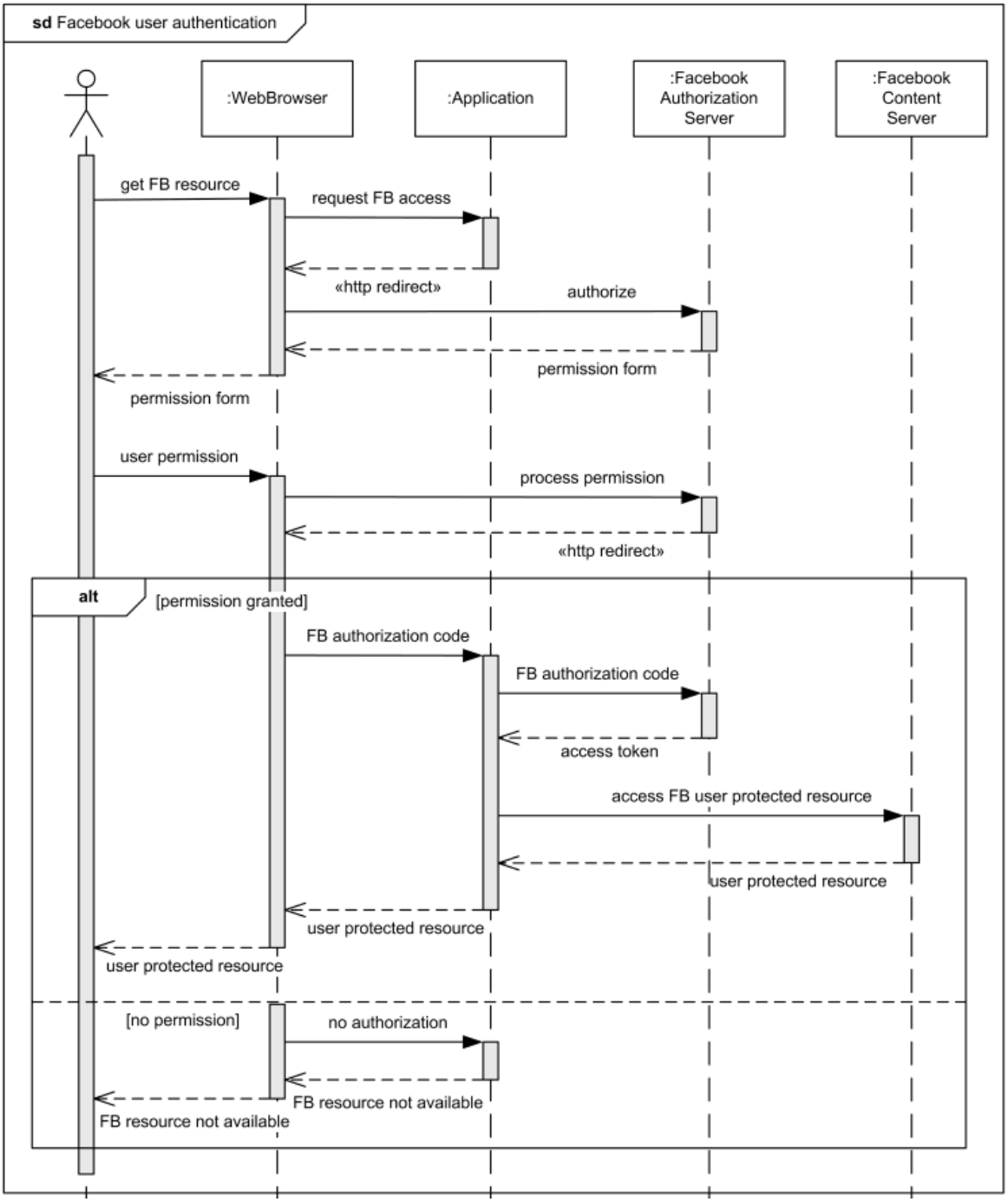
Expectation for solution: 4 class diagrams in total, each diagram at least 3-4 nodes (classes, interfaces, etc) and edges with meaningful relationships.

**Task 4**: Derive and draw a deployment diagram where you assume common architectures to run the browser, the application, authorization server and content server.

**Task 5**: Draw a state machine diagram for the authorization server. The authorization server is designed to defend the server against a brute force attack by limiting the number of requests per account per 15 min to 5. Attack model: the attacker sequentially tries entries in a data dictionary of most frequently used passwords like "12345", "qwerty", some profanities, some celebrity names, etc.

**Task 6**: Which of the architectural patterns (styles) presented in class would apply here? Discuss the one that you consider the best fit, argue why it fits, its benefits and drawbacks.

From http://www.uml-diagrams.org/sequence-diagrams-examples.html#facebook-authentication:




“An example of sequence diagram which shows how Facebook (FB) user could be authenticated in a web application to allow access to his/her FB resources. Facebook uses OAuth 2.0 protocol framework which enables web application (called "client"), which is usually not the FB resource owner but is acting on the FB user's behalf, to

request access to resources controlled by the FB user and hosted by the FB server. Instead of using the FB user credentials to access protected resources, the web application obtains an access token.
Web application should be registered by Facebook to have an application ID (client_id) and secret (client_secret). When request to some protected Facebook resources is received, web browser ("user agent") is redirected to Facebook's authorization server with application ID and the URL the user should be redirected back to after the authorization process.
User receives back Request for Permission form. If the user authorizes the application to get his/her data, Facebook authorization server redirects back to the URI that was specified before together with authorization code ("verification string"). The authorization code can be exchanged by web application for an OAuth access token.
If web application obtains the access token for a FB user, it can perform authorized requests on behalf of that FB user by including the access token in the Facebook Graph API requests. If the user did not authorize web application, Facebook issues redirect request to the URI specified before, and adds the error_reason parameter to notify the web application that authorization request was denied."