FOR EXTERNAL EXAMINER (date of this version: 20/3/2012)

UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

INFORMATICS 2C - INTRODUCTION TO SOFTWARE ENGINEERING

Wednesday 1st August 2012

00:00 to 00:00

Convener: J Bradfield
External Examiner: A Preece

INSTRUCTIONS TO CANDIDATES

Answer BOTH questions.

Both questions carry equal weight.

CALCULATORS MAY NOT BE USED IN THIS EXAMINATION

SOLUTIONS

FOR EXTERNAL EXAMINER (date of this version: 20/3/2012)

Problem 1

You are the technical lead in your company for a new product aimed at university research scientists: an electronic lab notebook (ELN). The marketing team has given you the following information.

> The scientists who will use the ELN traditionally record their experiments in paper notebooks, but increasingly they are looking for digital solutions which allow them to share their information with other scientists they are working with, such as Wikis and Dropbox, which make frequent functionality changes.
>
> A small amount of market research indicates that the scientists vary considerably in what the capabilities they would like in an ELN, and the ELN solution will need to change over time as the scientists' needs change. However the scientists all say an ELN should be easy to use and quick to use.
>
> The scientists work in labs headed by a senior academic (the Lab Head). Provision of computing resources for the lab (hardware and software) varies between labs. Some have all their needs met by the central university IT department; others manage all their own hardware and software and depend on central IT only for network connections; most are somewhere in between.

Answer the questions appearing on the following pages.

(a) Which software development process is likely to be most appropriate for developing the software system? Explain why, contrasting your choice with one other software development process. [*10 marks*]

XP or some other *agile* process. Positive reasons for an agile process include that the scientists vary as to what they want, the solution will need to evolve over time, the "easy and quick" requirement which is best approached iteratively, and the competitors mentioned (Wikis and Dropbox) which both change frequently. Negative reasons for not choosing another approach such as Waterfall, Spiral, UP, BDUF, etc, are that the requirements will be hard to pin down ahead of time because it is a diverse stakeholder group, there is no safety-critical aspect, the requirements aqre going to change over time.

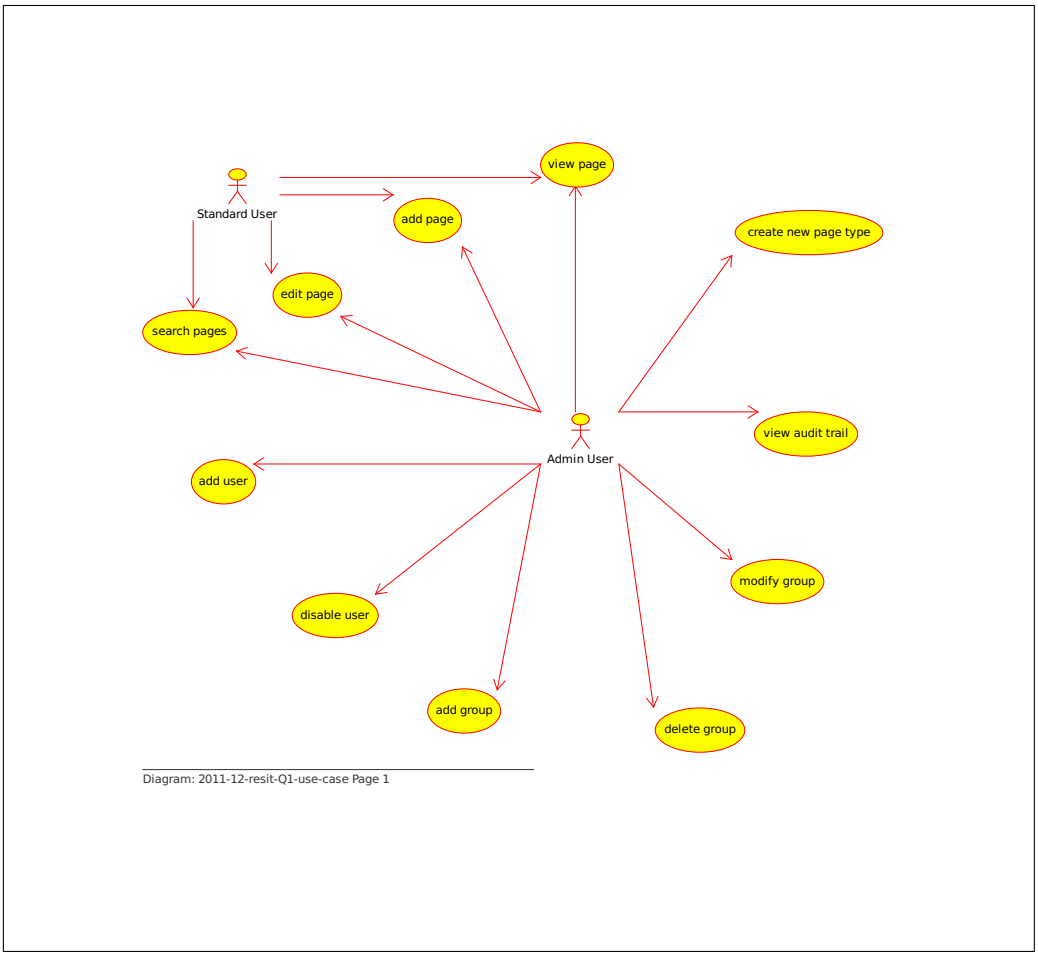
(b) Name three techniques you would use to gather requirements. Explain for each one what you would do for, who you would involve, why it is appropriate to use in this case, and any difficulties you might encounter. [*10 marks*]

Suitable techniques include interviews, scenarios (user stories, use cases), prototypes, facilitated meetings, observation. Of these the best are scenarios, prototypes, and observation. See SWEBOK chapter 2 for descriptions of each. 1 mark for each named, 1 for each what you do and with who, 1 why appropriate, 1 difficulties.

(c) Requirements elicitation methods have indicated the following system description:

> The ELN should be a browser-based web application. Users log on to gain access. User accounts are "standard" or "administrator". A "standard" user can add new pages, edit pages, view existing pages, and search for pages containing search terms. "Administrator" users can do everything a standard user can do and can also add new users and disable existing users. An administrator can also create user groups, and modify and delete them. And adminstrator can also view an audit trail of users' activity, and create new types of pages. The system must also include a messaging component that allows any user to send messages to other users or groups of users, view messages, and delete messages.

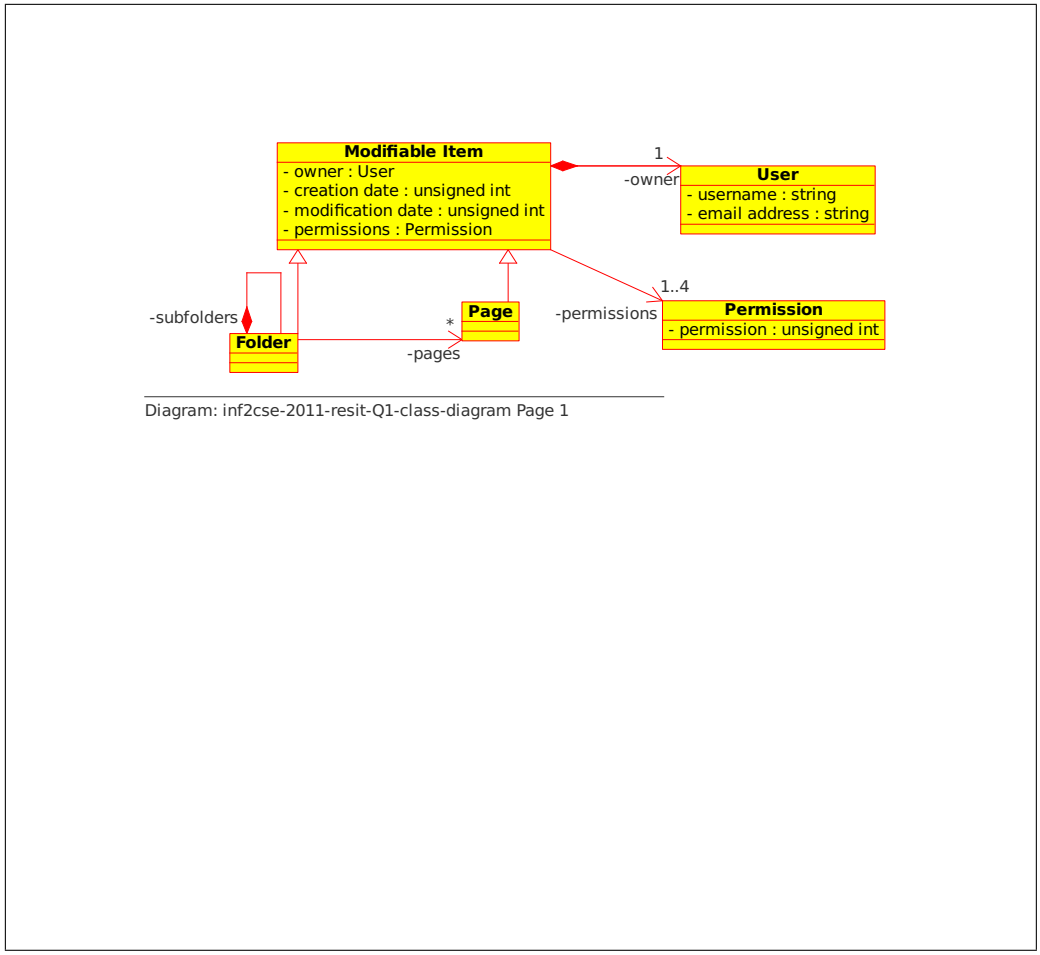
Supposing you had decided to use a formal process, draw a use case diagram for the system. [*10 marks*]



(d) Continuing with the supposition that you had chosen a formal process, you have designed part of the system as follows:

> Each *Folder* and *Page* has an owner (a *User*) and a non-empty set of *Permissions*. There are 4 kinds of permissions. Folders can have any number of Folders and Pages as children (making a tree structure). Each Folder and Page has a name and dates of creation and modification. A User has a username, a password, and an email address.

Draw the UML class diagram of this part of the system. [*10 marks*]



(e) Your development team consists of eight software engineers working out of two offices. One of the engineers proposes using the RCS system, another proposes SVN. What problem are they trying to solve with these systems? What model does each one use - name and explain? Which one of these two would you choose, and why? [*10 marks*]

RCS and SVN are source code control systems. The problem they deal with is how multiple developers can simultaneously work on the same code base. Doing this introduces the possiblity that changes may be subject to race conditions if two developers are working on the same source code file simultaneously. RCS uses Lock-Modify-Unlock - the file is locked, changes are made and submitted, and then the file unlocked. While it is locked, no other developer can do anything with it. SVN uses Copy-Modify-Merge - a local copy is made, changes are made to it, and then the changed file is merged back into the original. Multiple developers can do this simultaneously. The system can combine multiple modifications in many cases - if not then the potentially-conflicting modifications are thrown back to one of the developers to resolve. I would choose SVN for this project (an argument for a dVCS such as GIT is acceptable) - it gets developers out of each others way, and especially if they are working out of different offices they should be loosely coupled.

Question 2

(a) You are a member of the software engineering team working on proprietary software written in Java and using the JUnit regression testing framework. This is the first project you've worked on where the product has become sucessful in the market (all the previous projects were shelved or failed in the marketplace), and you are enjoying working on code that is in daily use, solving an important problem. Nevertheless, you are aware that a new competitor has entered the market and is doing very well - your product's position is under threat.

(i) You have found a security bug in the upcoming release of the product, a bug that is not present in the current version. Since use of the product involves entering personal financial details into a server, you are concerned that some customers could have their financial data stolen, although the bug is pretty obscure. The new version is to be released in three days, and marketing regards this release as crucial to maintaining market share. You know your boss will be angry if you bring this up now. Which section or sections of the ACM/IEEE Code of Ethics are relevant here (name each and give some detail of what it is about)? What are the arguments in favour of notifying your boss of this potential bug now? What mitigating factors might there be to keep quiet. [*10 marks*]

i. PUBLIC – Software engineers shall act consistently with the public interest.
ii. CLIENT AND EMPLOYER – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
iii. PRODUCT – Software engineers shall ensure that their products and related modications meet the highest professional standards possible.
iv. JUDGMENT – Software engineers shall maintain integrity and independence in their professional judgment.

All of the above are relevant. In favour: loss of financial data is serious for the individual, more than just a commercial decision; product/company will lose reputation for integrity if anyone loses financial data; commercial and emotional factors should now cloud professional judgement. Mitigating: the bug is obscure so the risk is actually very small.

(ii) You are browsing the competitor's public website and come across a page that describes a new feature they plan to introduce in their next release in three months. You think it must be an internal document that was never intended to be made public, although it is not marked "Private" or "Confidential" or the like. As you read, you realise this is a fantastic idea that will really appeal to customers, and you also realise that it could be added to your product in just a few days. But since this information was obviously not supposed to be released, you wonder about the ethics of using it. You quickly consult the ACM/IEEE Code of Ethics. What does it tell you? [*5 marks*]

It tells you that it is completely ethical to use the information. This information was made public by your competitor. There is no public interest argument, you are not undermining professional standards. It is a competitive market, information is valuable, companies should guard it.

(b) Your CEO has decided that the company needs to introduce a quality improvement process, so that over time she can be sure that the product quality is getting better. She asks you to look into it - she suggests ISO 9000 and CMMI as two to start with. You tell her right away that only one of these is suitable. Which is it? What is it about the other one that makes it unsuitable for her purposes? [*6 marks*]

CMMI is suitable. ISO9000 is not suitable because all it does is specify what sort of documents and procedures a company should follow in its quality control. It doesn't specify any particular level of product quality, or any method for improving product quality.

(c) You boss wants to focus the next release on security improvements.

(i) You are put in charge of this. You look at the Monster Mitigations from CWE. One of the principles is to: "Establish and maintain control over all of your outputs". What are the other four? [*4 marks*]

- Establish and maintain control over all of your inputs.
- Lock down your environment.
- Assume that external components can be subverted, and your code can be read by anyone.
- Use industry-accepted security features instead of inventing your own.

(ii) The product includes a component that accepts input typed in by the user and displays it back to the user on a web page. What should the component do to adhere to the principle given above? What can happen if the component does not do this? [*6 marks*]

The component should make sure that any special characters that will be interpreted by the browser are escaped or HTML-encoded. If this is not done, then carefully constructed input could include commands that the browser will execute, such as javascript.

(d) The product is a consumer oriented web-application that enables easier searching of retail websites such as supermarket sites. There is a new enterprise prospect (a large supermarket chain) in the sales pipeline. The sales team tell you that they are pretty sure this potential customer will want some statistics on reliabilty. Assuming the customer has a short attention span so you will only have time to provide one statistic, what would it be? Name it and describe it. [*6 marks*]

ROCOF - Rate Of oCurrence Of Failure. The number of times per minute/hour/day the system is unavailable. Mean uptime also acceptable.

(e) Your boss has read about an open source library that learns from shopper interactions what sort of products the shopper likes to buy. He thinks this would be a killer feature, and asks you to look into including it in the product. He says he thinks it might be LGPL'ed but he's not sure what that means or if he's right. What do you do? [*6 marks*]

Find out what the licensing terms of the library are. If it is GPL, it can't be used. If it is LGPL, it can be used. If it is some other open-source licence, then you need to check if it can be included in proprietary software.

(f) Your CEO is taking an unhealthy interest in the details of product development. She wants to know what the development team is doing about verification and validation, having heard these terms from one of the Directors of the company. First you have to explain to her what these mean. What do they mean? You explain that the JUnit test framework helps with both of them. How does it help with each of them? [*7 marks*]

Verification - are we building the software right? Validation - are we building the right software? Junit testing helps with verification in that it can verify that the software does what was intended if the test suite is comprehensive. It helps with validation if the test suite was designed in collaboration with the customer.