**題目: April 2014**

1. Please read this entire question before commencing to answer. Note that the inclusion of irrelevant information in answers may be penalized.

請注意，將不相關信息納入答案可能會受到懲罰。

Choose **one large-scale software project** you are familiar with.

(a) Provide **a brief description of the project**. You should explain **why you consider this to be a large scale project**, explain the **main purpose of the project** and **identify the main stakeholder groups in the project**. [6 marks]

Answer:

I think **Facebook obviously is a good large-scale software project** for this question. It maintains nearly 1.86 billion users to use their social network services normally and satisfyingly. Facebook collects a large amount of data about a user’s usage; their contacts, payments they make, the device they are using, and any information from associated companies. To keep this system working properly and can manage of increasing numbers of service requirements they build a high level software architecture which has large amount and various components. Firstly, Facebook use LAMP (Linux, Apache, MySQL, and PHP) as its basic structure, it is a stability and mature architecture structure. Meanwhile, Facebook modify and extend its operation to incorporate a lot of other elements and services to ensure availability. Such as in order to measure the site availability, Facebook measures potential errors, monitoring and fixing them before errors grow out of control. In addition, for these collected personal information, Facebook has developed a series of corresponding services for users to communicate with the social network such as user’s groups, user’s subscriptions and user’s payments. All the properties above indicates that Facebook is not only a quite large scale software project but also a good community site which can handle a lot of information and provide a wide range of services to hundreds of millions of users for using simultaneously.

**The main purpose of Facebook** like any other social media, they like to provide a social media service that continuously sustains 維持the user's interest and satisfaction. **The main stakeholder groups** would be like users who use these services, software developers who develop required functions, system architects who responsible to construct whole system and advertisers who promote their products on the website to interesting people, and that make Facebook gains quite profits to maintain the whole operation of website.

(b) Identify **two Quality Attributes of the system** that you consider to be important. You should **justify your choice** by providing an argument that the Quality Attributes are **valuable to particular stakeholder groups**. [8 marks]

Answer:

### **I choose **Availability** and **Security** as key quality attributes of the system. The reasons and explanations as follows:**

### ****Availability****

### Facebook has a huge number of users and the corresponding personal information in which the amount is increasing every second. In addition, the system of Facebook has to response millions of service requests and obtains the accurate data that users expect through the server. Therefore an ability of providing “always-on” application services and less tolerant of any service downtime has become very important for such a social media like Facebook. Otherwise the users will lose patience and confidence on the website and switch to another alternative websites because of always fault system and frequently wrong information. 缺點Poor availability can result in system cannot provide services while user makes a request. 優點By accounting for availability in the original architecture, system can shorten repairing time when errors occur and also can reduce the probability of errors occurrence to provide timely services for users. From those reasons evident that Facebook must take availability into account when designing every aspect of new features. This quality attribute is particularly valuable to the stakeholder groups like developing organization and maintenance organization because this is their responsibility, which is to construct a system architecture that can adapt with the user and data scale extensions and guarantee the system functions can work properly when errors occurrence, and also a ability of fast error repairing.

**Security**

Facebook collects a huge amount of data about a user’s usage. It is their responsibilities to guarantee that users’ data would not experience security risks during them enjoy the services. 缺點If the data were to be accessed by an unauthorised source then it could have serious implications for the user and Facebook. Other **potential sources of security risks** 風險來源comes from **cyber-attacks**, such as a denial of service attack. Since the Internet is full of a variety of information security threats therefore the functional aspect designs of security for Facebook system is particularly important. It must to develop sufficient security mechanisms to protect user data and itself. It is clear, due to its nature and size, that Facebook has a considerable range of potential security issues which it must take into account if it wishes to remain a trusted social networking site. **This quality Attribute is particularly valuable to the stakeholder groups** like developing organization, end user and customer becausedeveloping organization have to design a mature security system architecture and protection measures to protect users and customers.

(c) Provide **a quality attribute scenario** for your chosen system for one of your two chosen quality attributes. The scenario should **be realistic in the sense** that you can argue some of the stakeholders might require the system should pass the scenario. [8 marks]

### Answer:

### Scenarios in availability attribute:

1 the **source** would be **an internal function of the system** i.e. **messenger function.**

對該屬性可能產生影響的事件來源

2 the **stimulus** would be **a functional fault** of the system causes erroneous results i.e. **messenger unable to send message to other user.**

該事件對於系統可能造成的結果

3 the **environment** would be **normal operation**.

發生的事件的地點

4 the **artifact** would be **Facebook's massage service**.

該事件對於系統可能造成結果的對象(被刺激的對象)

5 A **response** would be when system notice an error occurs they would send a message to maintenance team to fix the error under a time limit.

該系統對於事件產生的結果所應該做出的反應

6 The **response measure** would be that the system would automatically test message function every 15 minutes to verify the function still alive and can send and receive all kinds of message properly. If the message function does not response in 15 minutes period, the system will inform the maintenance team to fix the error in a hour.

如何驗證該系統的屬性以驗證該情境式可以測試的

如果無法有效的規模化的後果If Facebook unable to provide availability for message function, users would become dissatisfied and find an alternative social media.

**Scenarios for security attribute:**

1 the **source** would be an increasing number of security threats **from the Internet** i.e. a high number of requests coming from the same IP address.

2 the **stimulus** would be that the service would be attacked i.e. a denial of service attack (as the site would be unable to defense).

3 the **environment** would be normal operation.

4 the **artifact** would be every Facebook's service.

5 A **response** to prevent cyber-attack like DOS is system provides a bandwidth over-subscription control (if the attacker can't fill the whole bandwidth it won't affect the site), or automated mitigation (by knowing the baseline traffic a site can redirect excess traffic, filtering out excess noise and passing on the clean traffic to the network). This response would change the mode of operation to ensure that normal service was still provided to trusted IP addresses.

6 The **response measure** would be that the system monitors the network traffic and analyze the source of suspect IPs every hour of every day. Once they identify the suspect behavior of IPs, they will block that IPs and report this finding to security team to do further investigation.

(d) Would the system you **have described pass or fail the scenario you described**? Justify your answer. [3 marks]

Answer:

### ****Availability****

Facebook provides a built-in function that every time you login your Facebook page the function will automatically check every service works properly and then turn off the service that you may not to use to enhance user experience. Therefore, the message function will answer the checking function’s call by sending an echo, and that can let system knows messaging function is ready for work. If the function detect errors or found no response from message function in certain time period it will send alarm to the maintenance team and ask them to fix the issue in limitation time. So, Facebook’s message function can definitely pass the scenario I previously described.

**Security**

Facebook applied a security mechanism for detection and blocking large amount service requests from suspect IPs. When they notice that there are huge numbers of request from the Internet, they will first active the load sharing mechanism to distribute the workload and then filter the suspect IPs from their behaviors to proceed later block. According to that network load control mechanism, Facebook can resist DOS attack and pass the scenario above.

2. You have been asked to develop the architecture for a web based system that is intended to help coordinate activities in emergencies (e.g. in severe ﬂooding, or after an earthquake or other natural disaster). Users include the emergency services (police, ﬁre, ambulance), volunteers and people in need of help. The system allows requests for tasks to be entered and these can be split into subtasks to be carried out by diﬀerent people and so on so that each task can be carried out in a coordinated way.

(a) Suggest an architectural pattern that is a good match for this system. You should justify your answer by pointing out two or three features that are well matched with your chosen pattern. [6 marks]

Answer:

An emergency online system that requires fast response capability would be very suitable for model view controller pattern because there are a lot of different views are required a variety of application needs. For example a fire incident occurs, the system has to different information to different reaction units such as to fire department the system has to provide not only the exact location of the incident but also the nearest location of hydrant nearby, and for ambulance unit the system has to provide the shortest path to the incident location and the number of injuries, etc. In addition, the MVC pattern has feature to break system functionality into three components: model, view and control. For model, it can provide specified data according to the request from controller. Besides, MVC creates different views for different user groups to implement that the information is purposefully be displayed. For controller, it manages the interaction between the model and the view, forwarding requests and processing requests. Therefore, MVC pattern is good candidate for such system which has requirements for continuing changed user interface of the application and has various user groups.

(b) Provide a diagram of your high-level architecture with a brief description of the role of each component. [6 marks]

Send query to DB

Answer:

Model\_Police

Return query result

State query

Model\_Fire

Model\_People\_need\_help

Model\_Fire

Response User request

Forward User request

Controller \_Police

View\_Police

View selection

Controller \_Fire

View\_Fire

Controller \_Fire

View\_Fire

Send User request

Controller\_People\_need\_help

View\_People\_need\_help

MVC pattern:

View:

Sending different user requests from different user groups to different Controllers e.g., police department needs the incident location and fire department needs the hydrant location and the incident location.

Deciding how to display the information based on the data transmit from Model e.g., only to show the information relative to the incident location to police department but indicates the resident’s basic medical information to ambulance unit in case people might get hurt.

Requests update from model.

不同的user會送給不同的controller,不同的controller會用不同的model去收

Controller:

It can use different Controllers to collect requests from different Views, which can efficiently classify the request into the corresponding business Model e.g., collecting requests from user of fire department to its specific Controller.

Define application’s behavior.

Forward the request to its Models.

Model:

Responses the specific request from specific Controller by sending query to the database to retrieve relative data e.g., the module responsible for handling the medical request will post a query request to the medical system database for medical information of the wounded.

Sending the retrieved data to the correspond View.

Notifies Views of changes.

(c) After an exercise in which the system failed for an hour at a critical point in the exercise it has been identiﬁed that availability of the system is critical. Identify **an appropriate architectural tactic** that could be used to improve availability of your system. Justify your answer. [4 marks]

Answer:

Fault recovery of availability tactic would be a useful choice for solving a situation likes above. Because such system that provides related information for medical rescue can only bear shorter time of system failure. Therefore, the best way to tackle this issue is deploy a redundancy function, once it notices the active system is suffering the critical situation or does not respond to request in a period of time it will automatically take over the control and sending the message to the corresponding systems for declaring its dominance, and sending an alarm to the correspond maintenance team to solve system failure.

(d) Provide brief notes, illustrated by diagrams if you feel this is appropriate, on how you would apply your chosen tactic to the architecture to ensure 99.9% availability (i.e. no more than around 1.4 minutes of down time in 24 hours of operation.) [5 marks]

Answer:

Controller\_Police

(Redundancy)

Send request

Forward request

Model \_Police

View\_Police

Controller\_Police

(Active)

Response User request

For example we can add this redundancy function into a controller and make them both connect to corresponding View and Model. In normal operation, only active controller will respond request and communicate between View and Model. The redundancy Controller will send a message in a time period to check the active one is alive and monitoring whether a fault has occurred in active controller. When it notices the active system is suffering the critical situation or does not respond to request in a period of time it will automatically take over the control and sending the message to the corresponding systems for declaring its dominance, and sending an alarm to the correspond maintenance team to solve system failure.

(e) Provide an argument to justify that your chosen approach could achieve the required availability. [4 marks]

Suppose you are working for a company that produces telephone exchange software. The software is responsible for responding to requests to make a connection, to establish the connection, maintain the connection and then terminate the connection at the end of the conversation.

(a) Identify two or three quality attributes that you think would be critical to the quality of the telephone exchange software developed by the company. Justify your choice in terms of the requirements of particular stakeholder groups. [6 marks] (b) Provide a brief description and justiﬁcation of an architecture you think would be appropriate for the static structure of the software. [3 marks] (c) Provide a quality attribute scenario for one of your chosen quality attributes. The scenario should be realistic in the sense that you can argue some of the stakeholders might require the system should pass the scenario. [8 marks] (d) Suppose that the telephone exchange software failed the scenario you have devised. What architectural tactic do you think would be appropriate to improve the chances of the telephone system passing the scenario. Justify you answer by demonstrating how the change could contribute to a change in outcome for the scenario. [8 marks]