**SD VCAA Sample Exam Questions 2011 – Sample Answers by**

**Kevork Krozian**

**Mark Kelly**

Questions are available at

 http://www.vcaa.vic.edu.au/vcaa/vce/studies/infotech/softwaredevel/IT-softwaredev-samp-w.pdf

**Question 1 – Mark**

- easy to use (since the general public will be using it)

- have strong data validation to ensure it is valid and complete (to avoid unintelligible data being entered that the system cannot interpret)

- be quick to use (so customers can enter their data promptly and be handled more quickly by staff)

- be cheap to operate and maintain (so money is not wasted)

- have a display that is clear and easy to read (so people with poor eyesight can read it easily)

- be secure (so people’s sensitive data is not accessible to unauthorised users)

**Question 1** – **Kevork**

 In general, behavioural user requirements are of one of two types: those that specify what is to be accomplished ( functional requirements), and those that specify how well the functions are to be accomplished ( performance requirements). <http://www.threesl.com/pages/webletter-February06/Non_Functional_Requirements.php>

Non Functional Requirements are (solution attributes) such as user-friendliness, response rates, robustness,

portability, reliability and maintainability ( p13 Study Design ). Therefore examples of Non Functional Requirements would include :

1. User friendliness of the User interface for a standard user which would be a customer
2. The response rates to user input
3. The robustness of the solution as far as how it handles unexpected user interaction
4. Reliability of the solution in the event of service difficulties or load levels that are beyond the usual
5. The ability to maintain the solution in the event there are changes to perhaps hardware or software
6. The ability to port the solution to a different environment
7. Availability of the solution in the event of high congestion levels

**Question 2 - Mark**

Layer 1 is the most primitive level of the OSI and is where hardware and data directly interact. Hardware opens data streams and channels incoming data to the layer 1 of another node. Streams are closed when data flows end.

Data arriving from the physical layer is directed upwards to higher layers where more abstract data operations such as encryption, packet handling and presentation occur.

**Question 2** - **Kevork**

**Ethernet operates at both Layers 1 and 2 so here is the first problem with the question**. Ethernet incorporates both the Physical layer and the Data Link Layer. <http://en.wikipedia.org/wiki/OSI_model>

As data moves down the layers it is progressively placed in larger “envelopes” or is encapsulated so the information is in the structure suitable for each layer ( see <http://www.infocellar.com/networks/osi-model.htm> ) eg. layer 3 “envelopes” are called packets with headers and trailers suitable for handling by layer 3 devices such as routers and layer 3 switches.

Layers 7,6, 5 have protocol data units or “envelopes” called “data” . Layer 4 is called “segment”. Layer 3 “packet”. Layer 2 is a “frame”. Layer 1 or the physical layer is “bits”.

The physical layer wraps up the information into bits for transmission across the medium ( cable, fibre, wireless ) . There aren’t actual bits moving but distortions along the medium that represent bits. Therefore, TCP/IP (TCP is layer 4, IP is layer 3 ) and Ethernet ( Layers 1 and 2 ) rely on the physical layer for the transmission of the information built at the higher layers. At the receiving node the package is decapsulated so that as it moves up the layers information is extracted from the next envelope within the previous envelope as each is opened . When the information reaches the top layer it is ready to provide information in the form for the application requesting or responding to the exchange or communication.

**Question 3 – Mark & Kevork both say…**

|  |  |  |
| --- | --- | --- |
| Function | Top | Output |
| Push 23 | 2 | Item added 23 |
| Push 18 | **3** | Item added 18 |
| Pop | 2 | Item removed 18 |
| Push 75 | **3** | **Item added 75** |
| Push 92 | 4 | **Item added 92** |
| Push 47 | **4** | **Stack full** |

Let’s assume that the events in the table are in chronological order. Push 23 occurred before push 18.

Let’s also assume that “Top” is a variable containing the value of the stack pointer: the current active stack position.

How does the table relate to the stack? We can only assume that the stack is shown as it is **after** the events in the table have been carried out.

We can only wonder why the bottom 2 stack items are **bolded**. The question does not explain this, and it not an ICT convention.

According to the table, after the PUSH 23, the stack pointer (“Top”) is 2.

In the stack, ’23’ appears in slot 3 (counting from both the top and the bottom).

Therefore if top’s value is 2 and it’s in position 3, we know the index number of the stack’s first slot is **zero**.

So the stack’s slots are numbered zero to 4, not 1 to 5.

If Top=1, and the stack is bottom-up, the current stack value is **83**.

The **next free slot** for a push is **Top + 1** (i.e. slot 2).

Apparently this stack updates the pointer immediately **before** a push/pop, rather than **after** it.

Other stacks update the SP (stack pointer) immediately **after** an operation.

The 23,75 and 92 shown in the stack **don’t actually exist yet** if you’re following the history of operations in the table.

At the start of the table’s events - before the push 23 - the stack actually looks like this:

|  |
| --- |
| **STACK** |
|  |
|  |
|  |
| 83 |
| 52 |

But it *may* finally explain the mysterious bolding of the 2 values in the question!

If we push 23, it goes into stack slot numbered 2 (the one physically third from the bottom).

TOP is updated to equal 2.

In the table, you can see the stack’s state after the push: top=2 and the output is “Item added (23)”.

In the next operation, PUSH 18, the value 18 is put on the stack in slot 3.

So in the table you fill in “3” into the empty cell.

The next operation is a POP so 18 is **removed** from the stack (which explains why the displayed stack does not show it) and the pointer is **decremented** (reduced by 1) to 2.

The next operation is a PUSH 75, so ‘75’ goes into slot 3 and the pointer is incremented to 3 again.

So we put “3” into the empty ‘TOP’ and the output would be “Item added (75)”

The next operation is a PUSH 92, so ‘92’ goes into slot 4 and the pointer is incremented to 4.

So the output to add to the table would be “Item added (92)”

The final operation, Push 47 causes a problem.

The stack pointer is already at its maximum value.

It cannot be incremented – in other words the stack is full.

The attempt to push 47 would, according to the explanation, result in the output “Stack full”.

The stack pointer remains unchanged.

Mark says - A lot of thinking for 6 marks! One hopes the real exam won’t have such a question with so many mysteries and vagaries that the poor student has to interpret before attempting to answer the question.

Kevork says - A much nicer way to introduce the question would have been to start with the following stack with no bolding

|  |
| --- |
| STACK |
|  |
|  |
|  |
| 83 |
| 52 |

And a statement that TOP is a pointer to the top of the stack and the capacity of the stack is 5 elements. All fixed

To summarise… a deskcheck:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Stack**  | **Starts at**  | **Push 23**  | **Push 18**  | **Pop**  | **Push 75**  | **Push 92**  | **Push 47**  |
| 4  |  |  |  |  |  | 92  | 92 |
| 3  |  |  | 18  |  | 75  | 75  | 75  |
| 2  |  | 23  | 23 | 23  | 23  | 23  | 23  |
| 1  | **83**  | **83**  | **83**  | **83**  | **83**  | **83**  | **83**  |
| 0  | **53**  | **53**  | **53**  | **53**  | **53**  | **53**  | **53**  |
| *TOP=*  | *1*  | *2*  | *3*  | *2*  | *3*  | *4*  | *4*  |

**Question 4 – Mark & Kevork both say…**

The Spam Act 2003 specifies that:

* **Unsolicited commercial electronic messages must not be sent.**
* Commercial electronic messages must include information about the individual or organisation who authorised the sending of the message.
* Commercial electronic messages must contain a functional unsubscribe facility.
* Address harvesting software must not be supplied, acquired or used.
* An electronic address list produced using address harvesting software must not be supplied, acquired or used.

Liam’s messages were unsolicited by his clients, therefore he is breaching the Spam Act and should stop his software sending the emails immediately.

**Question** **5 - Mark**

***a.***

- register users, allocate usernames and passwords and require users to login to the site

- use TLS or SSL to encrypt traffic between her site and her visitors’ browsers

- ensure her server has the latest security patches

- ensure she has current, reputable antivirus scanners running at all times

- use a quality router to protect her server from the internet

- run anti-DDOS software and appropriate tracking and logging software to identify and prevent attempted electronic intrusions

- use a reputable third-party payment service to handle orders using credit cards, Paypal etc.

- use Captcha technology to identify and reject non-human clients which may attempt to upload spam

- send a verification email to new users to which they must respond to ensure they (and not someone else) have given a valid and working email address

***b.***

To protect her site from being damaged.

To prevent her or her clients’ personal or financial information being stolen.

To give clients confidence that their information will be safeguarded.

**Question 5- Kevork**

A) I have no idea what the website looks like so I can’t explain why it is not secure. On the other hand to the general question, how can a website for ordering goods ( and assuming paying for them on the same website ) is the question security issues that must be considered include:

1. Ensure payment is made through encrypted connection - https: port 443 by default which is http ( port 80 ) with [SSL/TLS](http://en.wikipedia.org/wiki/Transport_Layer_Security) protocol to provide encrypted communication and secure identification of a network [web server](http://en.wikipedia.org/wiki/Web_server).
2. Register users possibly with verification to an email address from which a confirmation needs to be made before an order is accepted. This may be superfluous if the sequence of steps during ordering required payment information but could prevent wasteful interaction with the website by bots.
3. Ensure a good router with firewall is operating ( Not sure how the friend overseas can see the need for this by looking at web site )
4. Ensure good virus scanning is running on the web server ( again, how can this need be identified by browsing the web site )
5. Ensure client end validation is operating ( vs Server side validation of data entry ). This can be seen by viewing the source of the web page for any attempts to validate user entry eg javascript
6. Ensure latest server patches ( again, how can the presence or absence of this be established by a person browsing the site ? )
7. Perhaps use a “gateway provider” to provide a secure transaction such as paypal so that the transaction takes place within the secure site of the “gateway provider” by redirecting the payment part of the transaction there rather than trying to handle it within the same website.

 B)

1. To give the clients confidence the website and more importantly their financial information is secure. Once the reputation of a website is damaged it may effectively be unable to regain the trust of clients again.
2. To protect the business from loss of clients in the event of a security breach.
3. To protect the website/hardware/software/IT infrastructure from malicious damage

**Question 6 - Mark**

 a.

- many of the questions have options that are mutually exclusive (e.g. ratings of the college) so radio buttons would be an appropriate data entry control

- at least one field is of type date and should be stored in an appropriate variable type, and use an efficient data input control (e.g. calendar control)

- some fields should allow variable-length text data entry

b.

- radio buttons ensure valid responses and are quick and easy for the user to use

- using a calendar control is quicker than typing in a date

- using a rich text box control for text data entry allows the user to quickly edit (e.g. using copy/paste) and format text

**Question 6- Kevork**

A) The form allows for a level of validation by giving the option to select from a restricted list of answers ( eg. dates or tick boxes or radio buttons that point to short descriptions ). However, there is the scope to enter a unique answer by selecting the “other” option or answering the “why” section of a question. This would be a string or text data type

B). Taking this consideration of a restricted list of options will expedite data entry and processing because it can be computer processed and analysed as opposed to reading potentially a large number of unique answers to questions which then brings in the issue of interpreting, analysing and categorising the data.

**SECTION C**

**Question 1 – Mark and Kevork say…**

a. Retrieve competition information

b. Update match information *or* upload photographs

c. User code and password

**Question 2 – Mark & Kevork agree that**

a. If the <<extends>> were changed to <<includes>>, for the subscribers there will be no change: they will still receive their extra information.

b. The change would make the extra information available to all visitors, not just subscribers, and this does not fulfil the SRS’s requirement that the extra information is only available to subscribers.

**Question 3 – Mark & Kevork say…**

a.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User code | simone12  | 12simone  | 2simone  | 12simon  | 123simo |
| Correct format? | YESSubscriber codes starts with letter | NOName code too long | NONeeds an extra digit, or does not start with letter | YESValid 2 digits then 5 letters | NOThird character is not a letter. Not an official’s code not subscriber. |

b. It checks whether the first character is alphabetical, in which case the user is a subscriber instead of an official. If the first character is a letter, the usercode marked as valid and no further validation occurs. If it’s not a letter, it must be an official’s code and must be processed further.

c.

|  |  |  |
| --- | --- | --- |
| **User code** | **Value in *FormatCorrect* at end of algorithm** | **Explanation of value based on algorithm** |
| simone12  | True | First char is alphabetic so first IF is true and flag set to true in line 5 |
| 12simone | False | Char 1 not letter, so drops to length test and fails because it’s too long. |
| 2simone | False | Char 1 not letter, so drops to length test and passes. Countrycode = 2s. Namecode=imone.Countrycode is not numeric so it falls through to the return statement. |
| 12simon | True | Countrycode = 12 (numeric) , namecode = simon (text). This one is also flagged as True twice.  |
| 123simo | **True** | Length is 7, countrycode – 12. Namecode= 3simo. Countrycode is numeric so formatcorrect is set to true. Then fails namecode test, but has already wrongly been set to true. |

The question does not ask for a solution to the problem, but it could be repaired by changing

**If** CountryCode is Numeric **Then**

FormatCorrect True

**If** NameCode is Alphabetic **Then**

FormatCorrect True

**EndIf**

**EndIf**

to this

**If** CountryCode is Numeric **AND** NameCode is Alphabetic **Then**

FormatCorrect True

**EndIf**

Or this….

**If** CountryCode is Numeric **Then**

**If** NameCode is Alphabetic **Then**

FormatCorrect True

**EndIf**

**EndIf**

d.

i. They must be in alphabetical order. A binary search or chop can only work on a sorted list of values. Therefore the user codes need to be sorted first. In the case of subscribers, user codes will begin with letters but with officials user codes will begin with numbers. In the sorted list the codes of officials will come earlier as digits come before letters.

ii. Sorting – e.g. a bubble sort or quicksort.

**Question 4 - Mark**

This is a vague question: what are the examiners wanting to hear?

At the simplest, you could say:

- Assuming the software writes a log detailing the time of crashes, the state of the server at the time of the crash (e.g. a data dump) then the log could be read remotely to count how many crashes have occurred over time. If the number exceeds the target figure, the reliability of the website would be worse than it should be.

If the examiners wanted a more technical description, you could say:

- The software would be set to autorun on server startup. It would regularly write data dumps to disk containing as much information about the state of the system as it could. Deliberate system shutdowns would make the system write a “normal shutdown” entry to the log before the system went down. When the server starts, it would check whether the last log entry was “normal shutdown”. If it was not, it would indicate an abnormal end (‘abend’) and trigger the software to report the crash to the site manager (e.g. with an automated email alert). If the number of crashes exceeded the maximum allowed, a further alert would be raised to notify the site manager,

The question is not well worded.

**Question 4 – Kevork**

I am not sure where this website is being hosted . Is it external to the organisation or internal ? The only answer I can think of is a continuous checking that the website is up ( this can be done via a scheduled task running say every minute that checks that port 80 on the server is responding to external requests ) and logging this to a text or other type of output file. An analysis can then be carried out showing how many times the web server did not respond and for how long. A threshold may be used of say only count as “web site down” if there is no response for more than 10 minutes.

There could also be issues with the ISP that is outside the control of the WTU so if the website went down it may not be within their control. To separate these this possibility, internal ( within the LAN ) monitoring can also be carried out to see if the site is up assuming it is hosted within the WTU LAN.

**Question 5 – Mark**

**Issue:** Hackerscould try to access the server to use it to harvest information or use it as a host for a phishing exploit.

**Prevention**: scan the server regularly for illicit code or directories. Use a router to prevent port sniffing.

**Issue:** Officials’ passwords could be found out and abused by unauthorised people.

**Prevention:** force officials to change their passwords regularly.

**Issue:** Usernames and passwords could be captured in transit between the user and server. **Prevention:** Use SSL or TLS to encrypt passwords and usernames.

**Issue:** A brute force dictionary attack could be used to guess passwords.

**Prevention:** force users to use strong passwords that are not in a dictionary. Temporarily freeze accounts after a given number of failed login attempts.

**Question 5- Kevork**

Security issues to consider could be drawn from a long list

1. Use encryption for logging on so username and passwords are not sent in plain text
2. Up to date virus, spam, malware protection for the server
3. A robust firewall
4. Good password policy ( minimum strength, frequency of change, inability to use passwords again )
5. Prevent login and block accounts after 3 failures. Resets subject to stringent validation.