M15/4/COMSC/HP3/ENG/TZ0/XX/M

Diploma Programme
Programme du diplôme
Programa del Diploma

Markscheme

May 2015

Computer science

Higher level

Paper 3

8 pages

Subject details: **Computer science HL paper 3 markscheme**

Mark allocation

Candidates are required to answer **all** questions. Total 30 marks.

General

A markscheme often has more specific points worthy of a mark than the total allows. This is intentional. Do not award more than the maximum marks allowed for that part of a question.

When deciding upon alternative answers by candidates to those given in the markscheme, consider the following points:

- Each statement worth one point has a separate line and the end is signified by means of a semi-colon (;).
- An alternative answer or wording is indicated in the markscheme by a "/"; either wording can be accepted.
- Words in (…) in the markscheme are not necessary to gain the mark.
- If the candidate's answer has the same meaning or can be clearly interpreted as being the same as that in the markscheme then award the mark.
- Mark positively. Give candidates credit for what they have achieved and for what they have got correct, rather than penalizing them for what they have not achieved or what they have got wrong.
- Remember that many candidates are writing in a second language; be forgiving of minor linguistic slips. In this subject effective communication is more important than grammatical accuracy.
- Occasionally, a part of a question may require a calculation whose answer is required for subsequent parts. If an error is made in the first part then it should be penalized. However, if the incorrect answer is used correctly in subsequent parts then **follow through** marks should be awarded. Indicate this with "**FT**".
- Question 4 is marked against markbands. The markbands represent a single holistic criterion applied to the piece of work. Each markband level descriptor corresponds to a number of marks. When assessing with markbands, a "best fit" approach is used, with markers making a judgment about which particular mark to award from the possible range for each level descriptor, according to how well the candidate's work fits that descriptor.

General guidance

Issue	Guidance
Answering more than the quantity of responses prescribed in the questions	• In the case of an "identify" question read all answers and mark positively up to the maximum marks. Disregard incorrect answers. • In the case of a "describe" question, which asks for a certain number of facts *eg* "describe two kinds", mark the first two correct answers. This could include two descriptions, one description and one identification, or two identifications. • In the case of an "explain" question, which asks for a specified number of explanations *eg* "explain two reasons …", mark the first two correct answers. This could include two full explanations, one explanation, one partial explanation *etc*.

1. (a) A method designed to break/crack an encryption code/key / decrypt the key/code (**not** password);
By trying every possible combination; **[2]**
Note: *First mark can be awarded for "decrypts encrypted information" or similar.*

(b) It contains data about different mobile devices;
So that (downloaded) content can be adjusted/customised to suit the device / check if the phone is of a suitable standard to access the site; **[2]**

2. (a) *Award up to **[4 marks max]**.*
*Award **[1 mark]** for the example which deals with an appropriate area in the Case Study.*
*Award **[1 mark]** for making clear that **increasing** one will **decrease** the other.*
*Award **[1 mark]** for the security process involved.*
*Award **[1 mark]** for an effect on usability.*
*Award **[1 mark]** for an extended description of the consequence of this.*

Example: paying for coffee in a coffee shop;
If the process requires the entering of username/passwords/some kind of biometric factor which will increase security;
If the customer is going to use a smartphone to pay he/she wishes this to be a fast, uncomplicated process (usability), not the opposite;
The customer might decide that it is in fact easier paying by cash/credit card;

Example: authentication;
The use of out-of-band via a mobile phone as an additional layer of security;
This will increase the time required to make a transaction;
Which may well put the customer off using internet banking/make him change banks;
Note: *"Internet banking/mobile banking" requires some elaboration before the first mark can be awarded.*

Example: login procedure;
Increasing from one-factor to two-factor;
Two-factor is more secure but takes more time for the user;
One-factor is quicker for the user, but less secure e.g. if someone finds out your PIN; **[4]**

(b) Asymmetric encryption is necessary so that a session key/password can be safely exchanged / to authenticate the sender/receiver;
As this will be sent with a private key that can only be decoded by the intended recipient;
Once the key/password has been exchanged symmetric encryption can take place;
As this requires less processing (by server and client) and this allows transactions to be carried out faster; **[4]**
Note: *Award **[2 marks max]** for an understanding of the two methods of encryption.*
e.g. Asymmetric uses a public key to encrypt and a private key to decrypt: Symmetric uses the same key for both encryption and decryption. Do not award full marks if the reason for asymmetric is not given (session key transfer).

3. (a) Man-in-the-Browser is a type of Trojan/virus (any malware) that resides in browser/extensions/user scripts/code/embeds/attaches itself in the browser (**not** "webpage");
It modifies the onscreen content / modifies bank account details of the recipient in transactions / keyloggers after transactions; **[2]**

(b) *Award up to **[4 marks max]***.

Example 1:
Normal login process takes place *before* the modified data is sent so SSL does not prevent the attack;
SSL protocols/encryption takes place *after* the data has been modified so does not affect the attack / Authenticates the user not the data entered in the browser;
Out-of-band verification / Uses mobile phones (SMS messages from the bank)/ email/phone call;
To confirm the transaction with the legitimate user / spot the modified details;

Example 2:
Two-band/multi-band authentication will not prevent the attack;
Because MitB only changes the content not the login details / they may be keylogged;
Out-of-band verification / Uses mobile phones (SMS messages from the bank)/ email/phone call;
To confirm the transaction with the legitimate user / spot the modified details; **[4]**

4. *Areas that should be explored include:*

Technology

NFC

- Produces radio waves that operate in a short range.
- Powered by NFC waves (induction) generated by retailer's NFC chip: passive mode.
- Or by the phone's own power source: active mode.
- Passive mode only allows data to be sent / active allows two-way transfer (offers/coupons *etc*).

QR Codes

- A 2-D barcode that contains the user's account details.
- Software is well established.
- Scanned by the retailer's POS scanner / ATM's incorporated scanner.

Processes

- In both cases the user opens a "mobile wallet app" with a password.
- Payment service is selected.
- Either QR code is generated and scanned or phone is placed close to POS terminal (or "tapped").
- With NFC (Barclaycard for small amounts) phone can just be tapped on already prepared POS terminal with no prior steps taken by user.

Security

- Both methods remove the dangers of card-cloning.
- In both cases the account data can be stored in a "secure element" on the SIM card.
- Or at the financial institute's server / in the cloud.
- NFC signals can be picked up outside of the nominal range.
- QR code difficult to intercept without taking the phone.

Level of Acceptability – user

- No agreed way of incorporating NFC chips.
- Could be part of phone circuitry / incorporated into the SIM card / attached as a sticker.
- QR codes require no additional hardware on the client side / software generated.

Level of Acceptability – retailer

- NFC requires purchasing of additional hardware / costs.
- Without knowing that the technology will be taken up universally.
- QR codes require only the (already present) scanner.

Conclusion

- There needs to be a final conclusion based on the arguments previously presented.

Marks	Level descriptor
No marks	• No knowledge or understanding of the relevant issues and concepts. • No use of appropriate terminology.
Basic 1 – 3 marks	• Minimal knowledge and understanding of the relevant issues or concepts. • Minimal use of appropriate terminology. • The answer may be little more than a list. • No reference is made to the information in the case study or independent research.
Adequate 4 – 6 marks	• A descriptive response with limited knowledge and/or understanding of the relevant issues or concepts. • A limited use of appropriate terminology. • There is limited evidence of analysis. • There is evidence that limited research has been undertaken.
Competent 7 – 9 marks	• A response with knowledge and understanding of the relevant issues and/or concepts. • A response that uses terminology appropriately in places. • There is some evidence of analysis. • There is evidence that research has been undertaken.

Proficient
 	
10 – 12 marks
	• A response with a detailed knowledge and clear understanding of the relevant issues and/or concepts, including:
	  • *the processes and technology involved*
	  • *the level of acceptance of both customers and retailers*
	  • *security aspects*
	• A response that uses terminology appropriately throughout.
	• There is competent and balanced analysis.
	• Conclusions are drawn that are linked to the analysis.
	• There is clear evidence that extensive research has been undertaken.

[12]

Total: [30]