N14/4/COMSC/HP3/ENG/TZ0/XX/M

International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

MARKSCHEME

November 2014

COMPUTER SCIENCE

Higher Level

Paper 3

7 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.

1. (a) A zero-day attack is one that attacks a previously unknown (until being used); Weakness in a computer application/security system; ***[2 marks]***

(b) A man-in-the-middle attack occurs when an attacker is able to intercept packages between two users; Without either of the victims realizing that this is happening; ***[2 marks]***

2. (a) *Award **[1 mark]** for a description of a Botnet, and up to **[3 marks]** for a description of how they are used.*

A *Botnet* is a collection of computers infected with malware;
That are controlled by a third party;
Attacks specific server in a coordinated attack;
Large number of requests overwhelm the victim; ***[4 marks]***

(b) *Award up to **[2 marks]** for each advantage, up to **[4 marks max]**.*

Examples:

There is better security when students use the proxy server for internet access;
The server will have a customized firewall/updated anti-virus software *etc* to protect the network;
The server can cache web pages;
This reduces bandwidth/saves user's time;
The server can record/monitor activities;
Allowing an analysis of events if something unforeseen occurs;
The server can block certain websites;
To prevent students from accessing inappropriate content;
The server can hide the IP addresses of the devices inside the network;
Making it more difficult for these devices to be attacked from outside; ***[4 marks]***

3. *Answers may include:*

Success of many attacks depend upon social engineering.
Sites such as Facebook try to make clicking irresistible.
By introducing offers/faking friends' requests/appealing to "popularity ratings" *etc.*
Tweets can be sent via Twitter that contain malware.
Which can then be rapidly spread to "followers" (trending).
YouTube links can contain malware.
Some of the above links may cause malware to be introduced into the company's systems.
Most companies allow the use of social networking / Many make use of enterprise social networking.
The massive (real-time) distribution of data via social networking makes this medium an obvious choice for cyber-criminals.

Marks	Level descriptor
0 marks	No knowledge or understanding of the relevant issues
1–2 marks	The answer shows a limited understanding of the issue.
3–4 marks	The answer shows some understanding of why this threat exists, or only considers one area in detail.
5–6 marks	The answer references two types of social networking. The student shows a clear understanding of how the malware is introduced and realizes how the massive use of social networking and its use in the workplace contribute to the threat.

[6 marks]

4. *Answers may include:*

Legacy Firewall Systems

- Packet filtering
- Packets are inspected to see whether they comply with previously established rules
- With regards to source/destination address, protocol used, designated ports
- Typically checks the packet header
- Non-compliance results in the packet being dropped
- Stateless (inspected independently from other packets in the same stream)
- Stateful filters keep check of the state (type of connection) of a series of packets to prevent the passing of any "rogue" packet from that stream
- Application-Layer filters check the content at a "port" level meaning that they have "knowledge" of types of connections (e.g. HTTP).

Malware

- Reference may be made to any of the techniques referenced in the Case Study

Next-Generation Firewalls

- Provide deeper inspection looking for malware without latency
- Can check the complete stack
- Can check user's identity
- Allows incorporation of black/white lists
- Includes SSL decryption
- Can be finely controlled

IDS (Intrusion Detection Systems)

- IDS systems analyze the system's configuration with respect to its level of security
- IDS systems measure the response of a system to known patterns of attacks
- They are passive systems that report back on possible threats

IPS (Intrusion Prevention Systems)

- These systems actively intervene to prevent possible attacks from taking place
- They work in line behind the system's firewall(s)
- Make use of signatures and traffic analysis

Whitelisting

- This provides IPS systems with legitimate sites so that any packets sent from these sites will be allowed to pass into the network.

APTs (Advanced Persistent Threats)

- Involve the attempt to successfully break into a system and remain there undetected for a long period of time
- A variety of techniques are used including social engineering and spearfishing
- Once in, a backdoor is set up and admin rights are sought to allow software to be "legitimately" installed on behalf of the attacker
- Targets companies where large financial gains can be made

SIEM software (Security information and event management)

- Aims to provide a holistic view of a company's security
- System collects and logs data from all relevant sources (IPS, firewalls, virus programmes, servers, devices *etc*)
- Analyses data to look for anomalies
- APTs can be detected by analysing outgoing traffic
- "Normal" system parameters need to be input first
- Complex to manage ⇨ there are organizations that provide and manage these systems

Markbands

There must be evidence of independent research and investigation for students to reach the top level.

Marks	Level descriptor
0 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. • No reference is made to the information in the case study or independent research. • The answer may be little more than a list.
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 related 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. • A response that uses terminology appropriately throughout. • There is competent and balanced analysis. • There is clear evidence that extensive research has been undertaken. • Conclusions are drawn that are linked to the analysis.

[12 marks]

Total: [30 marks]