M14/4/COMSC/HP3/ENG/TZ0/XX/M

International Baccalaureate®
Baccalauréat International
Bachillerato Internacional

MARKSCHEME

May 2014

COMPUTER SCIENCE

Higher Level

Paper 3

12 pages

https://xtremepape.rs/

*This markscheme is **confidential** and for the exclusive use of examiners in this examination session.*

*It is the property of the International Baccalaureate and must **not** be reproduced or distributed to any other person without the authorization of the IB Assessment Centre.*

https://xtremepape.rs/

General Marking Instructions

1. Follow the markscheme provided, award only whole marks and mark only in **RED**.

2. Make sure that the question you are about to mark is highlighted in the mark panel on the right-hand side of the screen.

3. Where a mark is awarded, a tick/check (✓) **must** be placed in the text at the **precise point** where it becomes clear that the candidate deserves the mark. **One tick to be shown for each mark awarded.** When marking **Question 4**, use the Scoris underline tool to underline key parts, and then use the textbox tool to add a comment stating which band the response is in, as well as any supporting explanation.

4. Sometimes, careful consideration is required to decide whether or not to award a mark. In these cases use Scoris™ annotations to support your decision. You are encouraged to write comments where it helps clarity, especially for re-marking purposes. Use a text box for these additional comments. It should be remembered that the script may be returned to the candidate.

5. Personal codes/notations are unacceptable.

6. Where an answer to a part question is worth no marks but the candidate has attempted the part question, enter a zero in the mark panel on the right-hand side of the screen. Where an answer to a part question is worth no marks because the candidate has not attempted the part question, enter an "NR" in the mark panel on the right-hand side of the screen.

7. Ensure that you have viewed **every** page including any additional sheets. Please ensure that you stamp 'SEEN' on any page that contains no other annotation.

8. A mark should not be awarded where there is contradiction within an answer. Make a comment to this effect using a text box or the "CON" stamp.

https://xtremepape.rs/

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.

https://xtremepape.rs/

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*.

https://xtremepape.rs/

1. (a) The *threat landscape* refers to the range of malware/dangers/threats or any singular danger;
Award the second mark for a good expansion, for example:
(Classified based on) the level of risk / the number of attacks / origin;
That are (currently) putting IT systems/companies data/personal data/networks at risk; ***[2 marks]***

(b) *Whitelisting* refers to the production of a comprehensive set of websites/IP addresses/email addresses; *(Do not accept devices)*
Which are permitted to access the network/device / pass through the perimeter controls; ***[2 marks]***

2. (a) Malware can breach (the security perimeter in various ways (e.g. zero-day attacks, social engineering) in order to install code such as rootkits, trojans. These are not intended to damage the system or its files, but are designed to send confidential data out of the network. Security systems such as IPS systems can look for unusual patterns of network traffic leaving and flag that there is a security breach.

Award marks as follows, up to ***[4 marks max]****:*
The idea that malicious code can be installed;
Without being detected (either when entering or when in place);
Accept Stuxnet/Duqu as student clearly understands that they are relevant here;
Do not accept "virus".
And an explanation of what it does;
Do not allow if it deals with actions on the computer itself (ie. should include the possibility of data leaving the system).
The monitoring of data leaving to spot unusual patterns/suspicious packets;
The consequence of discovery e.g. send alert amends data log;
Do not accept "stops" or "prevents" on their own. ***[4 marks]***

https://xtremepape.rs/

(b) *Award marks as follows, up to **[4 marks max]**:*
*Award **[3 marks max]** for an explanation of how the attack is successful and an additional **[1 mark]** for a method of prevention.*
*Award a maximum of **[3 marks]** if the attack is incorrectly named (assuming the explanation and prevention are correct).*

SYN Flood
This exploits the TCP protocol (3-way) handshaking protocol;
Perpetrator sends the normal (SYN) message to the victim and the victim responds with a (SYN-ACK) message;
However the expected ACK reply does not occur;
Because of spoofed IP address etc.;
Many such requests are made at the same time using up server/system resources / leaves the connection half-open;
Prevention
IPS/Firewalls can filter these out (by inspection);
A time limit can be put on the 3–way handshake;

Smurf attack
Packets are sent to the broadcast address of the network being attacked;
This results in a copy of the packet being sent to each node on the network;
The source IP address is spoofed to be the address of the victim;
Which results in the reply packets being sent to themselves (echoed);
Resulting in bandwidth saturation (or equivalent);
*(Award **[1 mark]** for the idea of "successive" pings being sent)*
Prevention
Disable the IP broadcasting feature at the network router (accept firewall);

Stack-based Buffer Overflow
The (stack) buffer is deliberately supplied with more data than it can handle;
Can lead to overwriting of adjacent data (including the return call);
Which can lead to system crashes/resource exhaustion/infinite loops/an exit from the application (which causes DoS);
Prevention
The use of a "stack canary", which is a randomly chosen integer placed after the last valid space in the buffer. Before a return call from the stack is made, the integer value is checked. ***[4 marks max]***

https://xtremepape.rs/

3. *Award up to **[4 marks max]** for knowledge of an MitM attack, including SSL.*
*Award up to **[2 marks max]** for details of a method of attack:*

MitM & SSL
SSL allows the secure transfer of a (symmetric) key to be used in transfer of data (between 2 parties) / initiates a private/public key exchange / use of two keys;
SSL authenticates/confirms the identity of the site that is being contacted/accessed;

A (successful) MitM attack works by intervening/intercepting in the "conversation";
Allowing the data/message to be read/intercepted/modified;
Without either party realizing;

Attacks
*Award **[1 mark]** for a method of intercepting (e.g. breaking the key, setting up own SSL);*
*Award **[1 mark]** for how the attack is carried out.*

Example attacks:
SSL Spoofing
The original request (from client to server) is made with a HTTP protocol (ie. unencrypted). If this is intercepted then the attacker can set up its own SSL session with the server allowing all data/messages to be intercepted and messages to be injected (note: client's computer will **not** display a HTTPS connection).

CA Compromise
If the attacker gains a false CA (CA hacked / corrupt personnel) then he will have the private key associated with it, and can therefore trick the client into believing he is a legitimate site (e.g. client's bank).

Size of public/private encryption keys
Sites that continue to use small key sizes (e.g. <2048 bits) run the risk of their keys being broken due to the increasing processing power of modern systems. This would allow the private key to be compromised.

ARP Cache Poisoning
The ARP cache for a local network matches MAC addresses with IP addresses for each machine on the network. Cache poisoning involves altering the settings to replace a legitimate device with the attacker's.

DNS Spoofing
Similar to Arp Cache Poisoning, where the original DNS request is intercepted and responded to with the attacker's IP address. ***[6 marks]***

https://xtremepape.rs/

4. *The question addresses 3 related issues:*

- *Reasons for introducing a BYOD policy*
- *Concerns of the security personnel*
- *Measures that must be taken*

Reasons for implementing a BYOD policy

Consumerization

- This has led to the widespread ownership of smart / 3G / 4G devices
- Many employees will own at least 2 devices (smartphone and tablet)
- This allows them to connect to the company's network either
  - Internally via Wi-Fi, or
  - Externally via any Internet connection
- Employees prefer to use their devices than the company's because
  - They are more familiar with them
  - They can mix work and pleasure

Improved Efficiency

- A mobile workforce can work anywhere, anytime
- Allowing employees to use their own devices improves employee satisfaction

Lower TCO (Total Cost of Ownership)

- Companies do not have to supply the devices for the employees (or replace / repair them)
- This needs to be balanced against increased security costs

Security Concerns for implementing a BYOD policy

Employee owned devices will contain personal apps and data

- Some may be pirated or from dubious sources
  - Can have malware in them which attacks company data

BYOD will involve a large range of devices

- Each device will have different characteristics / OS
  - This multiplies the number and variety of threats as different OS present different vulnerabilities

Employee malpractice

- Some devices will be "jailbreaked" (iOS)
  - This can lead to a weakening/bypassing of the devices security mechanisms
  - Allows unapproved apps to be downloaded
  - Which may contain malware
- Android rooting
  - This can lead to a weakening/bypassing of the devices security mechanisms
  - Leaving the device vulnerable to attack

https://xtremepape.rs/

Sensitive company data will be stored on personal devices

- Workers can leave the company
  - If dismissed may use the data maliciously (e.g. Sold on to rival companies / blackmail)
- Devices may be lost/stolen
  - Data may be used maliciously sold on to rival companies

Control of the data is now more firmly in the hands of the employees

- Some employees may be untrustworthy
  - Leading to unauthorized access to data
- They might use unsecured Wi-Fi networks
  - Leading to unauthorized access through attackers listening in

Security Measures that can be taken

Implementing a comprehensive BYOD policy for all of its employees (Enterprise Mobile Management, EMM)

MDM (Mobile Device Management) software which manages the devices

- Enforces a common policy for all employee devices
  - Employees download a client programme
  - This checks the device configuration for minimum requirements
  - Checks device protection systems
  - Enforces upgrading / patching
  - Can lock down device
  - Maintains an inventory of all devices

MAM (Mobile Application Management) which manages the data

- Controls the access to company data for mobile devices
  - Enables the downloading of applications (includes company email)
  - Installs an app catalogue (dependent upon user access level)
  - All data is encrypted
  - Stores company data (including email attachments) in secure area (see below)
  - Allows remote wipes (lost device / employee leaves)
  - Geofencing capabilities (can suspend certain functions in certain areas)
  - Assigns apps/data access depending upon user access level (need to know)
  - Push capabilities (for sending notifications etc.)
  - Requires the use of VPNs
    - These private networks protect transmitted data by encrypting it
    - Each device appear to be a node on the network (even if remote)
  - Provides user authentication
    - Use of 2/multi factor authentication to identify user
  - Monitors and tracks the devices (depending on privacy policy)

https://xtremepape.rs/

Containerization (Sandboxing)

- Creates a separate area on each device
  - Containers can be deleted
  - Containers can be locked (if an attempt to copy etc.)
- That contains the companies data/apps
- Separates company data/apps from personal data
  - It is a mobile application(s) + data
  - Prevents malware, intruders, other apps etc. from interacting with the data

Using a VDI (Virtual Desktop Interface / Desktop Virtualisation)

- Data has a high level of protection
  - All within the company's perimeter
  - Firewalls etc. can protect the data
  - No concerns about employee neglecting security
  - Only screenshots, mouse clicks and keyboard strokes traversed the network
  - No sensitive data is ever on the employee's device
- Easier to update applications
  - Only one version in one place
- Can be complex to set up
- Can be frustrating for employees
  - Latency can be high
  - Often requires large screen, keyboard, mouse
  - Prohibits off-line working
- Can lead to high costs for networking and storage
  - All data stored by the host system
  - High network traffic as remote users

Note that the 3rd level bullet points (square bullets) are required to show a detailed level of understanding (10–12 mark band).

https://xtremepape.rs/

Award marks as follows:

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. ***M14 clarification:*** *The candidate gives a general response with minimum detail or understanding.*
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. ***M14 clarification:*** *The candidate gives a largely descriptive response which includes both the dangers* ***and*** *solutions; or an in-depth response on the dangers (****or*** *solutions), together with a reference to the rationale.*
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. ***M14 clarification:*** *The candidate shows a reasonable level of understanding of all 3 issues, or a detailed level of understanding of the danger* ***and*** *solutions, omitting the rationale.*
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. • Conclusions are drawn that are linked to the analysis. • There is clear evidence that extensive research has been undertaken. **The answer shows a detailed level of understanding.** ***M14 clarification:*** *The candidate shows a detailed level of understanding of the underlying computer science, shown by a balanced analysis of the 3 areas. Several examples and appropriate terminology are used.*

[12 marks]

Total: [30 marks]

https://xtremepape.rs/