Mana Tohu Mātauranga o Aotearoa
New Zealand Qualifications Authority

Level 3 Digital Technologies 2024

91908 Analyse an area of computer science

EXEMPLAR

Merit

TOTAL 05

[redacted]

INSTRUCTIONS

There are three questions in this assessment, on the topics of:

- big data (page 3)
- complexity and tractability (page 12)
- network communication protocols (page 20).

Choose only ONE question to answer. Copy and paste the name of the question you will answer in the box below.

Read all parts of your chosen question before you begin. Do not repeat your response in different parts of the question.

Candidates must complete their assessments individually under teacher supervision, in accordance with the NCEA Assessment and Examination Rules and Procedures. The material submitted for assessment must be the candidate's own work.

Candidates are not permitted to access any resources (either in hard copy or online) other than those supplied in the assessment itself.

Schools, teachers, and candidates are not permitted to share or discuss the assessment or their assessment responses with any other schools, teachers, or candidates until after the final date for submission (30 October 2024).

The use of chatbots, generative AI, paraphrasing tools, or other tools that can automatically generate content is not permitted and material generated by these tools should not be submitted as part of the candidate's work.

(Assessment Specifications, NZQA 2024)

[redacted]

OR: QUESTION THREE: Network communication protocols

The table below shows four layers of the internet protocol suite.

(a) Complete the table below by placing the correct protocol into each cell. Two of the protocols have been completed for you.

Protocols, Ethernet, IPv4, UDP, Wireless LAN, DNS, TCP, IPv6, SCTP, FTP, HDLC.

Layer	Protocol 1	Protocol 2	Protocol 3
[redacted]	HTTP	SCTP	FTP
[redacted]	TCP	UDP	TCP
[redacted]	IPv4	IPv6	DNS
[redacted]	HDLC	Ethernet	Wireless LAN

Source: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:the-internet-protocol-suite/a/the-internet-protocols

(b) Explain HTTP and HTTPS.

In your response:

- compare and contrast them
- highlight the implications for data transmission
- provide specific examples of how each protocol should be used.

HTTP and HTTPS also know as hypertext transpher protocol and secure hypertext tranfer protocol are both used in the transfer of data between servers and clients. HTTP being the older of the too works with unencrypted transition of the data while as HTTPS is encrypted. They both work in the application layer and do not do the sending of the data themselves but instead reliy on another protocol like TCP. HTTP/S formats the data with a header that allows of any recipient computer to easily analyse the data and decide what to do with it. The header is made up of the start line with includes the method, what data is being requested and the version of https. Methods are what HTTP/S use as commands when transferring data. This includes commands such as get (request a specific bit of data) put(Add data to the server like filling out a google form) and delete(Remove something from the server entirely. The next part of the header is information about the client such as the browser type and the user of the computer and the last bit is the body which holds the data being sent. Both HTTPS and HTTP use headers to send data. The main difference between HTTPS and HTTP are that HTTPS in encrypted while HTTP is not. HTTPS uses protocols like TLS and SSl to encrypt the message while it is being sent between client and server. TLS works by the client requesting a certificate of authentic from the server which if acknowledged is then sent to the client which can verify the authentic of the website so encrypted data can then be sent. When HTTP data is sent there is not encryption at all so the data can just be accessed as it travels through the internet. This is fine in the case of

[redacted]

simple websites and no information is being exchanged but when sensitive data needs to be shared such as passwords, personal information and credit card numbers HTTPS encryption is crucial for ensuring that your data can not be taken freely by anyone on the internet. This means that HTTPS is used by banking websites, online shopping websites and anything else where personal information is used. The main downside of HTTPS is a slower connection and load times as it has to verify both parties and encrypt the data however this trade off is almost always worth it. While HTTPS is not required it has become common place as any website without it will be flagged not secure by google and do worse in the search algorithm.

[redacted]

RESOURCE A

Encapsulation and de-encapsulation

[redacted]

Source: https://www.computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html

Refer to Resource A to support your response to part (c) below.

(c) (i) How are encapsulation and de-encapsulation utilised in network communication protocols?

Encapsulation and de-encapsulation are important components of network communication. They are essential for sending data as they the header and trailer hold the location of the data as well as the sender and the intended recipient. They are also used for error detection and correction with components like CRC and Checksums being stored in the encapsulation process.

(ii) Explain why they are important features of network communication protocols.

If encapsulation and de-encapsulation were not used then it would be very hard for computers to send and receive data and as they would not be able to send the additional information about the data that aids transmitting. Without encapsulation the only connections that would work would be direct line connections between computers and even then it would have large amounts of difficulty's. This is because common error checking like CRC and checksums would not work as they both add headers and trailers to data. For example CRC works by adding all the data together into a long binary string and then dividing by a selected polynomial and then adding the remainder know as the CRC remainder to the data in the trailer. The recipient then divides the whole equation by the same polynomial and if its remainder is zero it means most likely no errors have occurred. This would not be possible without encapsulation as it would not be possible to occurred. This would not be possible without encapsulation as it would not be possible to add headers and trailers to data. This would mean that it would be very hard to check data

[redacted]

for errors and lots of long-distance connections would fail as there would be too many errors. Encapsulation and de-encapsulation are also essential for send packets as it tells the recipient the orientation of the packets so they can be rearranged properly

[redacted]

(iii) What problems could occur at the **transport layer** and **network layer** of the internet protocol suite if a packet was not de-encapsulated?

If a packet of data was not de-encapsulated in the transport and network layer of the internet protocol suite their would-be significant errors. This would be because the sent data would have addition information along with the data that would not make sense. For example if the data still had the CRC remainder on it then it would have additional information that may come out as nonsense in the sent data if not separated from the data. This would likely result in the corruption of the data or the data being unusable. An other problem would be that the data might not be formatted properly for storage. For example the data would most likely be in a packet which means that its only a select section of data and needs to be reassembled to make sense. This means that if the data is not de-encapuslated it would still have the infomatoin about its packet orrintation which would not only not make sense in the application layer but also mean it was not reassembled correctly with its other packets in the right order. In short if a packet was not de-encapsulated it would most likely be coroupted and unusable for a multitude of reasons

[redacted]

RESOURCE B

'First in, first out' (FIFO) or 'First come, first serve scheduling' (FCFS) queuing

[redacted]

Source: https://book.systemsapproach.org/congestion/queuing.html

Refer to Resource B to support your response to part (d) below.

(d) (i) What would likely occur within the UDP protocol if UDP packets were to arrive at a FIFO or FCFS queue with no free buffer space?

Because UDP works by sending the data rapidly with little concern over its safety if a UDP packet reached a FIFO or FCFS queue that was lacking buffer space then the packet would most likely be deleted and the UDP simply not reach its destination. This is one of the main drawbacks of UDP as its lacks the ability to be able to check head of its destination and make sure that it will arrive at its destination.

😇 💢 👽

[redacted]

(ii) Explain the process that the TCP protocol would likely undertake if TCP packets were to arrive at a FIFO or FCFS queue with no free buffer space.

If a TCP packet were to arrive at a FIFO or FCFS queue with no free buffer space the TCP packet would also be deleted timing out. However, unlike UDP TCP has preventive methods to make sure that this doesn't result in the data never reaching its destination. When the TCP doesn't receive acknowledgement of its data being sent it would most likely just send the packet again where it would then hopefully reach its destination in one piece this means that the data would still be able to reach its destination and while an error had occurred it's not the end of the data.

(iii) Compare and contrast what the end user would likely experience at the application level if they were using TCP or UDP protocols for video conferencing and the FIFO or FCFS queue had limited buffer space.

When using TCP or UDP protocols for video conferencing and packet loss occurs the different protocols would result in different experiences at the application level depending on which protocol is used. TCP is connection based and would resend its data if it does not get acknowledgement that it arrived in one piece. This would result in a delay in the video and a pause where no new packets where sent. This delay would make the video call quality worse but not unusable as all information would still be sent. If UDP protocols where being used for the video conference, then instead of the UDP protocol sending the data multiple times when it doesn't get acknowledged it simply sends the next data packet. This would result in a gap in the videoconference where a frame of video and audio is missing but would not result in a large drop in quality as it assuming it was only one packet lost only a small pause would occur and no delay would take place. This is why UDP is typically used for real time applications like video calls or online gaming because it offers higher speeds and less problems when a packet is lost.

[redacted]

RESOURCE C

The CIA triad

[redacted]

Source: https://www.linkedin.com/pulse/cia-triad-joseph-stephen/

The CIA triad has three components: Confidentiality, Integrity, and Availability.

[redacted]

Source: https://securityscorecard.com/blog/what-is-the-cia-triad/

[redacted]

Refer to Resource C to support your responses to parts (e) and (f) below.

Secure sockets layer (SSL) and transport layer security (TLS) are foundational technologies for securing communications over computer networks. With the evolution from SSL to TLS, understanding these protocols is crucial for ensuring secure data transmission.

(e) (i) Explain the purpose of SSL / TLS and how it contributes to secure communications over the internet.

The purpose of SSL/TLS is to both authenticate the identity of the other party in a data transfer and then encrypt the data so it can not be accessed. This allows data transfer to remain secure and private and keeps personal information safe. Without SSL/TLS it would be very risky to send anything private or confidential over the internet as it would be unencrypted and assessable to anyone with the skills to glean it from the internet. This would result in a large amount of features on the internet being unusable such as having accounts, doing banking and buying things, and adding your information to a website.

(ii) Explain the process of a TLS handshake, including the steps involved and the purpose of each step. Be sure to mention the roles of certificates and keys in this process.

The TLS handshake is a method used to insure the security of a connection between a client and a server. The first step in this method is the hello message sent by the client. This hello message contains the version of TLS the client is capable of using as well as a random string of bytes. The second step occurs after the server resives the clients message sending back its own hello message. The servers hello message contains its authentication certificate which is used by the clients and verified with its public data base authenticating the server. Then the client and server create the private key they will use for the connection which involves the master key being sent first encrypted in the public key which the client has access to once the private key in held by both parties they both send finished encoded in the private key encryption which then allows the exchange of data to occur. This process meats all the CIA triad requirements and helps ensures a safe connection

[redacted]

(iii) Consider a scenario where an attacker is capable of intercepting and altering communications between a client and a server. Explain how SSL / TLS can protect against such an attack, specifically focusing on the aspects of confidentiality, integrity, and authentication.

If an attacker is capable of intercepting and altering communications between a client and a server then SSL/TLS will most likely be able to protect against the attack. If an attack has access to the connection between the server and the client but they are using SSL/TLS encryption, then the attack will only be able to see and edit encrypted data which would not be useful for the attack. The TLS handshake prevents any attacks because one a private key in initiated the client and the server are the only one that can decode any messages sent. The attacker can intercept and alter these encrypted communications, but this will not achieve anything as anything the attack removes or ads will not make sense when de-encrypted leading to an error. This ensures the integrity of the connection as neither parties information ends up being edited in a harmful way and the attacker can not access any private information from both parties as they lack the encryption key. This ensures the confidentiality and integrity of the connection.

[redacted]

(f) Critically analyse how network communication protocols contribute to ensuring the confidentiality, integrity, and availability of data within a connected environment. You may discuss areas from your studies were maintaining the confidentiality, integrity, and availability of data during network transmission is important.

You can use the options below as prompts, or you can discuss an area that you have studied in class:

- quantum computing
- artificial intelligence (AI)
- edge computing and IoT
- 5G technology
- blockchain technology
- machine learning in security.

Network communication protocols contribute to ensuring the confidentiality integrity and availability of data within a connected environment. An example where we can see this is in online shopping and e-commerce. Online shopping uses network communication protocols such as TLS encryption and TCP to ensure a safe and fast online shopping experience. TLS encryption and its handshake authentication method are essential for maintain confidentiality in online shopping. This is because of all the sensitive data that is exchanged in the process such as the address of the person, the bank account/ credit card number of the client and their personal details. If unencrypted a hacker could easily access and abuse the client's information and have an extremely negative affect on them. The authentication step of the TLS handshake ensures that the server is legitimate with its SSL certificate which means the authentication requirement of the CIA triad. The TLS handshake and the SSL certificate also are essential for ensuring the integrity of the product. The SSL certificate sent form the server authenticates the server when compared with the public record which ensures for the client that the connection is legit and not an imposter of phishing style attack. With out the SSL certificate lots more people would lose their information and money to phishing attacks where people impersonate other webpages and servers. This is how the SSL certificate ensures the integrity of the server and integrity of the connection. The availability is ensured by algorithms such as the ones used in the network layer. TCP ensures avalabity because if there are blockers or missing data packets the system will try again and make sure the data is error free. This ensures that the data is efficient at all times even when there are problems with the network which means that the e commerce websites are available at all times

Merit

Subject: Digital Technologies

Standard: 91908

Total score: 05

Question	Grade score	Marker commentary
Network communication protocols	M5	The candidate provided a clear and accurate explanation of key concepts and technical understanding. They gave a detailed explanation of how SSL/TLS protocols protect data integrity and confidentiality through encryption and secure handshake mechanisms. They also explained the role of these protocols in ensuring that data remains confidential and integral during transmission. The discussion on network communication protocols showed an understanding of the technical capabilities and limitations, which meets the basic requirements for a Merit grade, but did not extensively cover the broader implications or innovative aspects of these technologies. Examples like online shopping and e-commerce were used to illustrate how SSL/TLS enhances security. This application to real-world scenarios demonstrated an understanding of how theory applies in practical contexts. However, the examples and explanations could benefit from greater detail or discussion of contrasting scenarios or perspectives, which might have elevated the response to a higher Merit or to Excellence level. The response showed some comparative analysis, especially in explaining the importance of TLS over non-secure connections. However, this comparison was quite straightforward and lacked a deeper exploration of contrasting perspectives or alternative technologies. While the paper touched on important aspects of security protocols, it lacked insightful conclusions about future developments or deeper implications beyond the immediate context. The analysis was more describing than explaining. This submission could have been improved by discussing emerging security challenges or new technologies and evaluating different security approaches. This would have allowed for a deeper discussion of the strengths and weaknesses of existing protocols.