**COMP1002 – Assessment 1: Set Exercises**

Section 1 – Question 1

The patient passport will provide patients access to their health records digitally via the NHS app. It will allow users to be able to book appointments, order prescriptions and view test results and records. It will keep a track of every record a patient has and give any GP, pharmacy, NHS hospital and social care agencies access to these records. This will allow for better and more efficient health care provided to patients. However, storing every customer record in a wide database requires huge security measures to keep the data safe. If the data is not secure enough, it could involve in huge data leaks of every customer record that exists on the database. I have analysed the security requirements below:

Confidentiality

(Data confidentiality: How can businesses protect their data?, 2023) Confidentiality ensures that the records for each patient must be kept confidential from anyone that should not have access to the data. This means that only the patient, GPs, pharmacies, hospitals and social care agencies should have access to these records. The data in these records include medical history, test results and prescriptions. These records need to be protected during the transmission of the data and whilst it is being stored in the system. It is extremely important to keep this data confidential to protect patient privacy and to comply with regulations, such as the GDPR. Potential threats against the confidential information that is stored could be sabotage by employees, phishing attacks and malware. Interception of the data whilst it is being transmitted is also another threat to the data. The threats could lead to a loss of trust from patients using the system, which will affect the reputation of the healthcare providers and would have legal consequences.

Integrity

(Sluzki, N. 2023)Data integrity guarantees that each record is maintained accurate and unchanged to provide GPs and hospitals with up to date information of the patient. This means that the data integrity needs to be managed to not only keep the data safe but to keep the patient safe, which ensures the patients trust in the system. If any of the data has been intercepted and changed or modified, it could result in the wrong treatment or diagnosis. This would further lead to health complications for the patient and legal issues for the company as they have not ensured the safety of the data and the patient. The data needs to be kept unchanged and accurate during storage and after transmission. Threats of this happening are malware, system errors, unauthorized modifications of data and even human error. The consequences of this are incorrect patient data which means that patients could get the wrong diagnosis. This would lead to further consequences such as incorrect treatment plans and legal issues for the healthcare providers.

Availability

(*What is system availability?,* 2023) Only authorised users should be able to access the patient passport and it should be available to them whenever they need access to it. They will need to access patient records, any appointments made by patients and prescriptions ready to be collected. If patient records are not accessible or available then it could have serious consequences of delayed treatment for patients and missed appointments which would create a further backlog. The different threats that could cause the system to be unavailable are DDOS attacks, natural disasters, network issues and software errors.

Authentication

(Message Integrity Checks, n.d.)The system should have an authentication mechanism in place which will be used to verify the users that are accessing it. It should ensure that only the authorised users are accessing the system, meaning that if the authentication is not strong enough, unauthorized users may access confidential patient information. Strong authentication can be implemented by using muti-factor or biometric authentication, which will greatly reduce the risk of unauthorised people trying to access patient data.

Authorization

(Aakriti, 2023). Users of the system should only be authorized to access specific data and perform certain actions that they are supposed to do and access. This means that anyone who is unauthorised to system or should not have access to specific data on the system should not be able to access it at all. For example, patients should only be able to access their booking appointments, prescriptions and their own medical data but doctors should be able to access all of their patients’ medical history so that they can give them the right treatment as soon as they need. If the system isn’t secure with the correct level of authorization, it puts all of the information at risk with patients and doctors being able to access information that they shouldn’t, which could lead to data being leaked and attack on the system.

Accountability

(Aakriti, 2023).Even though security on the system may be set up correctly, the activity needs to be monitored to stop any attacks from happening and to keep logs as evidence so that any attacks can be traced. The risks of this not being implemented are threats or attacks from authorised users and no evidence of where the attack has come from. Any threats can be easily prevented if they are monitored and would save the healthcare providers a lot of money as someone could take the entire system down one day without anyone suspecting anything and with there being no evidence of activity.

Section 2 – Question 2

The communication between the healthcare provider and database can be built using either TCP or UDP. As (BasuMallick, 2022) states “(TCP) is defined as a connection-orientated communication protocol that allows computing devices and applications to send data via a network and verify its delivery”. The key difference between TCP and UDP is that TCP needs to “verify its delivery” and UDP “without verifying its delivery”. For TCP, this means that the server and host will directly make a connection first using a three way handshake. The direct connection will ensure a reliable connection as the packets will be sent in the correct order and without any errors; whereas UDP is unreliable and packets may arrive out of order or be lost (Yasar, 2023). UDP is more simple and easy to implement than TCP which makes it better for applications that can tolerate some packet loss, such as broadcasting, online gaming and DNS. It also has no flow control which means that the receiver could be overwhelmed with data. TCP has got flow control and pipelining, which improves the performance of the transfer(Assmann, 2023).

So, which transport protocol would be better best for healthcare providers to communicate with the database? The main priority would be to keep the data secure during the transfer but it also needs to be accessed as quick as possible. Both protocols have many different vulnerabilities as they were not made for security (Risk, 2021). Even though UDP may provide a lower latency and reduced overhead, the unreliability of data transfer increases the risk of the data being lost. Therefore I believe that TCP would be better suited for the transfer of patient data because even though it may have a higher latency, it provides reliability in delivering the data. It offers a good balance between performance and security as data will not get lost during transfer and will arrive in order. This means that healthcare professionals can access the data as soon as they need without any information missing.

There are many different tools used to identify potential bottlenecks within the network. I will explain what they are and how they are used:

The first tool that could be used is ping. Ping is used to find out the latency. If you write ping and the IP address or domain name in the terminal (for example, ping <https://www.youtube.co.uk/>) , you can see how long it will take to send and receive 4 packets (Pramatarov, 2024). If the number is any higher than about 100ms, then the latency is high which means there could be a potential bottleneck in the network.

The second tool is traceroute. Traceroute “tracks the route packets taken from an IP network on their way to a given host” (*Troubleshooting latency using traceroute, N.D*). It will get the latency the same way as ping does, however it also traces the route of the packets from the client to the host. Getting the exact route of the packets will give us the position of where the bottleneck is occurring (BH, N.T. 2023). It is done by writing traceroute and then the IP address or domain name in the terminal (for example, traceroute https://www.youtube.co.uk/), which will give you the latency and hop number. The hop number displays each point on the route. It returns the IP address of each hop as well as the latency which will tell you where the bottleneck is.

The next tool used is bandwidth testing. Measuring the bandwidth on the network will gather the speed of the data that is sent and received over the network. If the speed is lower than usual then it could mean that there is a potential bottleneck in the network (Lamberti, 2023). You can do this by using any speed testing app such as “speedtest.net”. You have to click start and it will measure the download/upload speed and latency. Depending on your internet service provider (ISP), anything under 20 mbps for download speed could indicate a bottleneck.

Another tool that is used is Wireshark. Wireshark is a network protocol analyser that is used to analyse networks and debug any issues that may occur such as bottlenecks. It allows the user to get the exact location of bottlenecks by “capturing and dissecting packets” (Alberts, 2023).

Conclusion

In conclusion, my analysis has provided a variety of security requirements by using CIA and AAA, which highlights the threats posed to the security of the patient passport and the consequences that they could lead to. I have compared TCP and UDP network protocols to gather the pros and cons for each, which has led me to decide on the most effective protocol for building the communication. I considered the balance between performance and security of delivering the data, which led me to choose TCP as it offers reliability. To identify bottlenecks within the network, I explained how to use specific network analysis tools, such as ping and traceroute. The security requirements, choice of network protocol and network analysis tools have been analysed effectively so that a secure and efficient patient passport system can be created.

Bibliography

Assmann, B. (2023) *HTTP keep-alive, pipelining, Multiplexing & Connection pooling*, *HAProxy Technologies*. Available at: https://www.haproxy.com/blog/http-keep-alive-pipelining-multiplexing-and-connection-pooling#:~:text=With%20pipelining%2C%20the%20browser%20can,in%20front%20of%20them%20complete. (Accessed: 21 February 2024).

BasuMallick, C. (2022) *Differences between TCP and UDP*, *Spiceworks*. Available at: https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/ (Accessed: 21 February 2024).

Risk, E. (2021) *TCP VS UDP: When to use which protocol*, *Twingate*. Available at: https://www.twingate.com/blog/tcp-vs-udp (Accessed: 21 February 2024).

Yasar, K. (2023) *What is Transmission Control Protocol (TCP)?: Definition from TechTarget*, *Networking*. Available at: https://www.techtarget.com/searchnetworking/definition/TCP (Accessed: 21 February 2024).

Alberts, S. (2023) *Wireshark: A powerful tool for cybersecurity analysis*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/wireshark-powerful-tool-cybersecurity-analysis-shanneece-alberts#:~:text=By%20capturing%20and%20dissecting%20packets,diagnosing%20problems%20efficiently%20and%20effectively (Accessed: 02 March 2024).

*What is system availability?* (2023) *Fiix*. Available at: https://fiixsoftware.com/glossary/system-availability/#:~:text=System%20availability%20(also%20known%20as,it%20needs%20to%20be%20used (Accessed: 06 March 2024).

*Data confidentiality: How can businesses protect their data?* (2023) *Penneo*. Available at: https://penneo.com/blog/data-confidentiality/ (Accessed: 06 March 2024).

*Message integrity checks: Detecting tampering with authentication codes* (no date) *FasterCapital*. Available at: https://fastercapital.com/content/Message-integrity-checks--Detecting-Tampering-with-Authentication-Codes.html (Accessed: 06 March 2024).

Sluzki, N. (2023) *Data Integrity Testing: Goals, process, and best practices*, *IBM Blog*. Available at: https://www.ibm.com/blog/data-integrity-testing/ (Accessed: 06 March 2024).

Aakriti (2023) *Comprehensive guide: AAA Framework in Network security- 2023*, *Network Kings*. Available at: https://www.nwkings.com/aaa-framework-in-network-security (Accessed: 06 March 2024).

Pramatarov, M. (2024) *What is Ping Command and how to use it?*, *ClouDNS Blog*. Available at: https://www.cloudns.net/blog/what-is-ping-how-to-use-ping/ (Accessed: 06 March 2024).

BH, N.T. (2023) *Traceroute: A crucial tool for monitoring network performance*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/traceroute-crucial-tool-monitoring-network-performance/ (Accessed: 06 March 2024).

Lamberti, A. (2023) *Network speed vs. bandwidth vs. throughput: What’s the difference?*, *Medium*. Available at: https://medium.com/obkio/network-speed-vs-bandwidth-vs-throughput-whats-the-difference-247cf03e3473 (Accessed: 06 March 2024).

*Troubleshooting latency using traceroute* (no date) *Troubleshooting Latency Using Traceroute - Sugar Support*. Available at: https://support.sugarcrm.com/knowledge\_base/troubleshooting/troubleshooting\_latency\_using\_traceroute/ (Accessed: 06 March 2024).