Section 1: Cybersecurity Analysis Using CIA and AAA Models- Alfie Nurse

---

CIA Triad

The first part of the CIA triad is confidentiality: “confidentiality measures are designed to prevent sensitive information from unauthorized access attempts”[1]. Therefore all confidentiality measures that are relevant to this app will involve safe-guarding medical records, test results, and personal identification details from unauthorised access.

Specific confidentiality techniques and procedures:

- **Data Confidentiality with Encryption -** The implementation of strong encryption to data both at rest and in transit will improve confidentiality, technologies such as AES for database encryption and TLS for secure data transmission could be incorporated. AES-256(Advanced Encryption Standard 256-bit) is often used due to its strong cryptographic security. TLS(Transport Layer Security) provides a secure channel between 2 communicating parties, such as a web browser and a server. Encryption converts the data into an enciphered format (ciphertext) that unauthorised people cannot understand without the decryption key, this means that even if it’s intercepted during transit the data is still protected.
- **Privacy:** Strict data access policies should be employed to ensure that the user’s data is only accessible by authorised parties (e.g doctors). These may take the form of Access Control Lists(ACL) which is a list of access control entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied, or audited for that trustee/person. Alternatively you could use Role-Based Access Control (RBAC) which is a set of rules used to control access to network resources, specifying what resources are allowed to be accessed by users or system processes, as well as what operations are permitted on given resources, such as: files, directories, network ports, or database records.

Integrity:

Integrity is the second part of the CIA triad it refers to how “The consistency, accuracy and trustworthiness of data [is] maintained over its entire lifecycle.”
[2]

Specific integrity techniques and procedures:

- **Data integrity:** Implementing Checksums or Hash Functions for data files verifies that information has not been altered or corrupted in transit. Before data is stored or transmitted, a checksum or hash function value is generated, this checks if the data has been altered during storage or transmission by comparing its pre and post-transfer

---

[1] WhatIs. (n.d.). What is the CIA Triad? | Definition from TechTarget. [online] Available at: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA#:~:text=The%20CIA%20triad%20refers%20to.

[2] Ibid

values. Cryptographic hashes (e.g, SHA-256) could also be used to verify that patient data has not been altered unauthorisedly. The use of these techniques ensures the accuracy and trustworthiness of the data by preventing man in the middle attacks.

- **System Integrity:** Implement regular system audits to check for and rectify system vulnerabilities; use an intrusion detection systems (IDS) to monitor the system and create alerts when a potential security breach happens; and make use of patch management protocols to ensure that software is up-to-date and to maintain the system's functionality and protect against unauthorized changes.

Availability:

Availability, in the CIA triad means that "Information should be consistently and readily accessible for authorized parties".
[3]

Specific availability techniques and procedures:

- **Redundant Systems and Data Backup:** Implementing redundant systems to provide operational continuity by having alternate resources e.g. backup servers and ensuring that regular data backups occur to preserve data integrity and facilitate recovery is fundamental to ensuring availability, these measures ensure that services remain accessible even in the case of a system failure.
- **Load Balancing:** Load balancing techniques which are techniques that distribute network or application traffic across multiple servers to prevent overload on any single server can prevent any single server from becoming a bottleneck and reduce the risk of system overloads. This ensures that the NHS app remains responsive, even during peak usage times, by efficiently managing traffic and resource utilisation.
- **DDoS Protection and Mitigation**: Protecting against Distributed Denial of Service (DDoS) attacks which flood services with excessive traffic, aiming to overwhelm and take them offline is critical for maintaining the availability of online services. Implementing DDoS protection measures strategies designed to absorb or deflect the impact of these attacks can help prevent or mitigate the impact of such attacks, ensuring that the NHS app remains accessible to users at all times.

AAA Model

Authentication is the process of verifying user identities to give them access to confidential information, such as a user's personal details. Authentication is mainly done with passwords, but could also include biometrics, security tokens, and two-factor authentication methods.

Authorisation checks user rights to access resources. It's crucial in cybersecurity to ensure users can only access data and perform actions according to their roles and permissions, often

[3] Ibid

managed through Role-Based Access Control (RBAC). RBAC defines and enforces access policies, aligning access rights with job functions.

Accountability tracks user actions, implement it with digital signatures for non-repudiation, ensuring actions in the app are verifiable and indisputable.
Maintain comprehensive access and audit logs that record user activities, ensuring actions can be traced to individual users for accountability, non-repudiation(guarantees message origin, prevents sender's denial of sending), and forensic purposes(Identifies data tampering, e.g., email authenticity.)

Section 2: Networking Analysis - Alfie Nurse

For the secure exchange of data with a ‘sensitive nature’ between healthcare providers and databases, HTTPS is an ideal solution, ensuring data integrity and confidentiality via TLS/SSL encryption. For transferring large and sensitive files, SFTP or FTPS are recommended, providing powerful security features including encryption and secure authentication, crucial for handling data-intensive medical records.

To answer the bottleneck question, the following information learnt from the "Lecture 4 - Transport Layer" PowerPoint can be used:

Understanding the principle of congestion control is crucial. Congestion in this lecture is defined as "too many sources sending too much data too fast for the network to handle". The manifestations of congestion include lost packets due to buffer overflow at routers and long delays from queuing in router buffers, which are top problems in networks.
The "congestion control" approach in TCP is described where the sender increases the transmission rate (window size) probing for usable bandwidth until a loss occurs. The control strategy includes:

Additive increase: The sender increases cwnd by 1 Maximum Segment Size (MSS) every Round-Trip Time (RTT) until a loss is detected.

Multiplicative decrease: If a loss is detected, the sender cuts cwnd in half.
Using these principles, network analysis tools such as Wireshark, also mentioned in the module can monitor for symptoms of congestion like multiple retransmissions and timeouts, which suggest a bottleneck. Additionally, the presence of "triple duplicate ACKs" can indicate packet loss and potential congestion in the network, prompting a fast retransmit without waiting for a timeout. By analysing the patterns of these indicators, the NHS can infer where the network is experiencing bottlenecks and address them accordingly.