CYBR 271 SECURE PROGRAMMING 2023
STUDENT NAME: Thomas Green STUDENT ID: 300536064

PART TWO – STRIDE

1. Data flows

Data flow	***Type of Threat***	***Description***	***Mitigation***
1.	Tampering	Attackers alter maintenance data during transmission over the network, compromising flight safety. Communication to the web application happens via HTTP, lacking encryption for data in transit which makes it vulnerable to attackers to modify data during transmission.	Strong encryption like HTTPS must be applied for data transmission between the office and web app, ensuring secure transmission. Implementing checks like digital signatures or hash functions is essential to validate data integrity, preventing tampering during transit.
2	Tampering	Malicious individuals manipulate maintenance records, endangering data accuracy and aircraft safety. Tampering with data from the API server to service application might disrupt processing, leading to unauthorized access and system instability. Attackers can change schedule for maintenance causing disruption in operational flow	Use encryption protocols such as TLS and SSL to encrypt data in transit, prevent attackers from intercepting and modifying data, safeguarding integrity and flight schedules and operational flow
3	Tampering	Maintenance crew interfaces with the Legacy Web Application within the data center environment. Malicious actors exploit vulnerabilities by manipulating HTTP requests or tampering with cookie values present in the legacy web application. From here they can circumvent the authentication mechanisms in place, granting unauthorised access to enable them to modify maintence task configuration	Deploy Intrustion Detection System (IDS), to continuously observe network and application activities, detecting anomalies or suspicious patterns. When potential tampering attempts occur, administrators are alerted. This approach not only safeguards checklists but establishes a baseline for normal behavior. Any changes from this baseline will also initiate alerts for investigation and mitigation
4	Tampering	Adversaries might alter part data, posing risks to aircraft safety. They manipulate data being sent or received by Service Application, leading to incorrect instructions, maintenance actions or system failures	Implement data validation to ensure part data accuracy. Use digital signatures to verify the legitimacy of critical part information. Enforce strong authentication and two-factor authentication for Maintenance Crew members and Service Application to prevent unauthorized access. Employ digital signatures to safeguard data during transmission, ensuring its integrity and authenticity

1	Information Disclosure	Attackers may attempt to gain access to sensitive maintenance records and proprietary information, potentially leading to exposure of aircraft maintenance procedures and policies	Implement role-based access control to ensure that only authorized personnel with specific roles can access certain records. This prevents unauthorized individuals from accessing sensitive information, as they will not have the necessary permissions. This will reduce unauthorised exposure and tampering with information
2	Information Disclosure	Data exchanged between Service Application and API server is currently transmitted in plaintext without encryption which poses as a security risk. Attackers with access to network traffic can intercept and read sensitive information being transmitted.	Implement strong encryption for data transmitted between service application and API server. Employ transport layer security (TLS) to ensure data is encrypted during transmission. Uses encryption algorithms to scrame data before it is sent and deypts it at receiving end.
3	Information Disclosure	Risk of lost or stolen devices result in exposure of maintenance records and personal data. Due to tablets lacking proper security measures regarding google ID and password and having no lock screen, this enables attackers to extract sensitive data, to be used to exploit the company	Ensure tablet storage is safeguarded through encryption and enable remote wipe functionality. Can also carry out routing security audits and testing on tablets and service application to identify and rectify vulnerabilities.
4	Information Disclosure	Sensitive data is vulnerable when transmitted via unencrypted HTTP connections, posing a risk of interception by hackers monitoring network traffic. Attackers exploit legacy app vulnerabilities to access maintence records and operational data, leading to information disclosure	Implement HTTPS for communication between Office and web-application. This ensures encryption of data in transit, preventing unauthorized interception. Regularly update and patch legacy web app to eliminate security vulnerabilities. Deploy intrusion detection systems to swiftly detect and thward unauthorised access attempts
1	Denial-of-service	Attackers launch coordinated DoS attacks on the API server and service application, overwhelming them with malicious traffic. This disrupts communication, causing service unavailability due to resource overload	Use traffic filtering to identify and block malicious traffic patterns. Employ rate limiting to control the number of requests from a single source within a specific time. Validate requests strictly and use intrusion detection systems to quickly spot and counter potential threats

2	Denial-of-service	Attackers overwhelm Legacy Web Application with a flood of requests or exploit its vulnerabilities, causing it to slow down, become unresponsive or crash. Disrupts access for legimate office staff or maintenance crew.	Utilise load balancing and reduncancy techniques to distribute traffic and ensure continuous availability. Employ a Web Application Firewall (WAF) to filter incoming traffic and thwart malicious requests, thus minimizing the impact of potential DoS attacks
3	Denial-of-service	Individual within office support team takes actions against company interests. Launches denial-of-service attack against Legacy Web Application, employing a number of tactics including pushing overwhelming requests to exhaust the application's vital resources such as memory, CPU and network bandwidth. This causes the web application to lose responsiveness	Create channels for communication for employees to voice concerns or grievances without resorting to malicious measures. Imperative to establish a incident response plan to address potential indie threats and DoS attacks.
4	Denial-of-service	Resource-intensive operations may render tablets unresponsive, hindering essential maintenance tasks	Enhance application efficiency through optimisation. Prioritise critical tasks to prevent resource drain. Utilise tablets with adequate hardware resources to ensure smooth data flows and counteract denial-of-service risks within scenario

2. Data stores

Data stores	***Type of Threat***	***Description***	***Mitigation***
Data centre database	Tampering	Attackers target data center database, where critical aircraft records are stored. Threat of tampering would allow unauthorised individuals to gain access where they manipulate data, introduce inaccuracies and potentially altering aircraft records. This leads to service application providing false information to maintenance crews	Implement stricter acess controls and data integrity measures. Access should be restricted to authorised personnel who have the necessary privileges. Enforcement of authentication methods like strong passwords and two-factor authentication to prevent unauthorised access can also be implemented. Regularly audit and monitor database changes also makes it harder for unauthorised users to gain entry and monitoring helps rollback unauthorised changes
Tablet database	Tampering	Malicious actors forge maintenance personnel's signatures in Tablet Database, allowing	Deploy robust authentication mechanisms for maintenance personnel, utilising multi-factor authentication where

Data stores	***Type of Threat***	***Description***	***Mitigation***
		incomplete or inadequate maintenance tasks to be falsely approved. This fraudulent activity compromises the accuracy and integrity of maintenance records	possible. Utilise digital signatures for tasks approvals, ensuring non-repudiation and authenticity. Enforce strict separation of duties, requiring multiple authorised individuals to approve critical maintenance tasks, preventing unauthorised single-person approvals and reducing the risk of falsification
Data centre database	Information Disclosure	Data centre database is vulnerable to threat of information disclosure. Attacker gains unauthorised access to database due to weak access controls and lack of encryption. Attacker exploits vulnerabilities to extract customer data, financial records and other critical information.	Enforce strong authentication mechanisms such as multi-factor authentication (MFA), which requires users to provide multiple forms of verification before access.
Tablet database	Information Disclosure	Information disclosures through application data collections can be manipulated by potential attackers to reveal sensitive data that might compromise the integrity of maintence operations. Given the tablets role as a tool for service, this can be used for benefit of an attacker, as they can exploit the application data, where they can access, location, time, identity and email.	Exert control over installation of applications on tablets. Policy should dictate that only work-related applications are installed with periodic reviews to remove unnecessary or non-essential apps.
Data centre database	Denial-of-service	Adversaries leverage vulnerability by inundating the data center with data packets flooding the system. This imedes the data centers capacity to opertatie at optimality and causing delays and distrumptions in functionality.	Implement traffic filter. This allows the system to ensure that only relevant data, directly related to aircraft operation and organization is allowed to access the data center. Non-essential data packets are intercepted and redirected away from data center.
Tablet database	Denial-of-service	Attacker engages in network jamming tablet database, sending data packets to overload communication channels. Effects synchronisation between tablet data base and central data center, causing operational delays and restrain service applications core tasks	Implement intrusion detection system (IDS) to monitor network traffic. Identify abnormal patterns indicative of network jamming attempts. Monitoring enables rapid response and mitigation to neutralise attackers efforts before they lead to significant disruption

3. Processes

Processes	***Type of Threat***	***Description***	***Mitigation***
Legacy Web Application	Spoofing	Attackers craft deceptive login pages that mimic legitimate interface of application, designed to trick users into entering in credentials without second guessing. Pushes emails to employees through phishing emails. Once attacker has access to credentials, they harvest the sensitive information to exploit it to gain access to the system	Integrate training for both crew members and office staff to be aware of threats such as these. Knowledge about tactics employeed in spoofing attacks, individuals become equipped to recognise these signs. They learn to differentiate authentic login interfaces from deceptive ones, identifying discrepancies.
API Server	Spoofing	Attackers attempt to deceive the system by falsifyfing API requests to impersonate legitimate tablets. Through manipulation, they can gain illicit access to sensitive aircraft data, undermining operational integrity and even compromising flight safety creating significant risks	Assign unique API keys or tokens to each tablet to ensure only authorised devices can interact with API server. Incorporate protocols like OAuth to strengthen identify verification. Implement IP whitelisting for API access, permitting requests only from trusted sources to safeguard against unauthorised access attempts.
Service Application	Spoofing	Unauthorized user impersonating exploiting vulnerabilities, attackers might gain entry to maintenance records, putting processes and flight safety at risk. Attacker aims to manipulate the applications trust in user identities and the integrity of task completion records.	Employing multi-factor authentication, as recommended, can verify genuine users. Enhance security using digital certificates or biometric authentication. Monitoring user access patterns helps support suspicious activity early. Regular security assessments and penetration testing can uncover and address vulnerabilities proactively.
Legacy Web Application	Tampering	Attacker intercepts HTTP request exchanged between user and application while initiating an order. Attacker exploits interception to modify critical details, including adjusting jobs and work specifications. This manipulation aims to undermine integrity resulting in inaccuracte records and work	Implement TLS encryption (HTTPS). Server as a cryptographic protocol so when data is exchanged during HTTP requests, rendering inctercepted data unreadable to unauthorised entities. By adopting HTTPS, the organisation safeguards the integrity of information transmitted during processes

Processes	***Type of Threat***	***Description***	***Mitigation***
API Server	Tampering	Attackers manipulated API payloads meant for the API server. This lead to unauthorised changes or actions within the system, jeopardising aircraft data and operations, causing data integrity and confidentiality to be compromised. Attackers could have the capability to insert harmful data or commands resulting in inaccurate application behaviour, unauthorised access to data and potential data leakage	Implement a robust encryption mechanism for data transmission, especially when itilizing the REST protocol. Utilise HTTPS to ensure that data sent between the API server and other components is encrypted and protected from eavesdropping. This is important since REST-based communications are over open web
Service Application	Tampering	Unauthorised modification of maintenance tasks. Threat involes attackers attempting to alter maintence tasks, potentially compromising aircraft safety and maintenance efficienty. Manipulation exploits vulnerabilities in the service application leading to discrepancies and hazards.	Implement Web Application Firewalls (WAFs) as they serve as a protective layer that can detect and block malicious code injections and tampering attempts before they reach the service application.
Legacy Web Application	Repudiation	Accountability denial when attackers perform unauthorised actions in Legacy Web Application and subsequently deny involvement. Creates complexities in accuracy attributing specific actions to individual users which hinders the organisations ability to establish proper accountability	Implement robust auditing and logging mechanisms within the Legacy Web Application. Record user actions, system interactions and activities. Maintiaining comprehensive logs, the organisation can construct an audit trail that effectively tracks and verifies user activities, ensuring accountability
API Server	Repudiation	Attacker intentionally disown responsibility for generating an excessive influx of API requests. Requests are intented to overwhelm API server capacity, leading to service disruptions and degradation. Reupdiating involvement the attacker seeks to evade accountability	Implementing API throttling mechanism acts to reduce impact of excessive requests. Involves imposing limits on rate and volume of API requests that a user or application can generate within a timeframe. Organisation establishes a safeguard against consumption of server resources
Service Application	Repudiation	Maintenance Crew member carries out an action within application. Member updates	Require approval from two authorised maintence personnel using biometric or multi-factor authentication for

Processes	***Type of Threat***	***Description***	***Mitigation***
		status of task only to deny involvement with it later. This creates uncertainty which could lead to challenges in accountability tracking and confidence in the integrity of actions taken within the application	secure task acknowledgment. Adds extra layer of verification, preventing situation such as falsely denying completed avionics system inspections
Legacy Web Application	Information Disclosure	Attacker uses vulnerability of path traversal to access unauthorised information that would necessitate valid credentials for retrieval. By exploiting this vulnerability the attacker can manipulate paths to traverse through directories to gain access to sensitive data, compromising integrity and confidentiality of the application	Implement stringent input validation and sanitisation mechanisms within the codebase of the application. This helps filter out path manipulation, which can help the application thwart attempts to exploit traversal vulnerabilities.
API Server	Information Disclosure	Exposure of unguarded configuration files containing sensitive information are accessible to external parties. Attackers can exploit this vulnerability to gain insight into server settings, architecture and other potential vulnerabilities.	Employ awareness to developers about the importance of securing configuration files. Awareness of the consequences of file exposure and make aware the necessity of safeguarding sensitive information. Implementation of access controls at file system level can also restrict unauthorised access to configuration riles. Role-based access control mechanisms can ensure files can only be accessed by authorised personnel
Service Application	Information Disclosure	Attackers may exploit vulnerabilities in service application to gain unauthoritised access to confidential information related to aircraft maintence, records, checklists and manuals. This breach of security could lead to unauthorised parties obtaining insights into procedures, potentially compromising the integrity of maintenance operations	Implement strong user authentication mechanisms, including multi-factor authentication (MFA), to ensure that only legitimate users can access servive application. Authroisation mechanisms should be integrated to allow access to relevant information based on roles and permissions
Legacy Web Application	Denial-of-service	Attacker exploits vulnerabilities in authentication mechanism by repeadly guessing user credentials or tokens. This could potentially overwhelm the application’s authentication	Implement rate limiting mechanisms to restrict number of login attempts within a specific time frame, preventing attacker from executing guesses in a short period. Implement account lokout policies that temporarily

Processes	***Type of Threat***	***Description***	***Mitigation***
		protocols, causing degradation of service or complete availability	suspend user accounts after a certain number of failed attempts have been made by the same IP address
API Server	Denial-of-service	Malicious actors push a high-volume of convincing HTTP requests directed at the API server. The quanitiy of requests overwhelms the server's resources, such as CPU and bandwidth, resulting in a slowdown of complete unresponsiveness of the API server, distrupting essential function of data synchronisation for tablets	Implement intrusion detection and prevention systems (IDS/IPS) that can identify abnormal spikes in incoming request rates. Utilise load balancing techniques to distribute incoming traffic across multiple server instances, preventing any single instance from becoming a bottleneck
Service Application	Denial-of-service	Group of actors initiates DoS attack on Service Application for financial and personnel gain. These threats encompass scenarios involving brute-force login attacks and "Ping Flood" attacks. These malicious actions aim to overload the applications resources, leading to unavailability and inconveniencing legitimate users, thereby distrupting critical maintenance tasks.	Implement CAPTCHA challenges into high-risk areas of the application, such as login pages or areas prone to being attacked. This helps differentiate between human users and bots attempting attacks. Implement architecture of service application to be capable of dynamically distributing traffic across multiple servers. Load balances can help distribute load and mitigate impact of a sudden increase of requests
Legacy Web Application	Elevation of privilege	Malicious actor identifies a weakness in application, specifically a flaw that enables the manipulation of URL parameters during the login process. Seizing upon this vulnerability, the attacker modifies these parameters, effectively tricking the application into bestowing them with administrator priviledges. With access to these permissions, the attacker breaches the authorised boundaries of access, potentially compromising the integrity of our maintenance protocols	Employing role-based access control (RBAC). Implementing it in the buisiness provides a formidable barrier around the Legacy Web Application. This approach ensures that even if an attacker manages to exploit a vulnerability, their actions remain confined within the limitations of their designated user role.
API Server	Elevation of privilege	Attackers have potential to steal API keys, to impersonate legitimate personnel and	Adopt tokens like JSON Web Tokens (JWT) instead of simple API keys. JWTs are short-lived tokens with build-in

Processes	***Type of Threat***	***Description***	***Mitigation***
		manipulate the API server. This can lead to unauthorised actions and compromise security protols.	expiration, limiting their usefulness for extended periods. Ensures that even if a token is compromised it will only be viable for a limited time, reducing potential impact of unauthorised access attempts.
Service Application	Elevation of privilege	Threat of tablet authentication bypass, where malicious actors attempt to circumvent the authentication mechanisms on the tablets. This could enable them to gain access to maintenance records and perform actions that are not authorized	Regularly updating and patching the Service Application is crucial to address any known vulnerabilities and minimize the risk of exploitation. Additionally, implementing strong authentication mechanisms on the tablets, such as biometric or PIN-based authentication, can help prevent unauthorized access attempts. Employing secure coding practices and encryption to protect sensitive data stored on the tablets enhances overall security.

4. Interactors

Interactors/Actors	***Type of Threat***	***Description***	***Mitigation***
Office Support	Spoofing	Attackers craft convincing emails posing as office support staff, tricking employees into malicious actions. Emails sent contain urgent maintenance tasks, containing deceptive links which lead to harmful sits. These threats exploit recipients trust and jeopardise organisational security	Implement email filtering solutions to work as a frontline defense. These solutions identify and intercept phishing emails ensuring they never reach employer inboxes. Also implement email filters that examine content, links and attachments, that recognise malicious intent, preventing employees from interacting with altogether harmful information
Maintenance Crew	Spoofing	Attacker gains access to maintenance crew area and gains access to crew member login credentials via a sticky note. Attacker uses these credentials to impersonate crew member, gaining unauthorised access to service application and gains information for personal benefit	Implementing 2FA adds additional layer of security. Even if attacker manages to obtain login credentials they will still require a second form of verification. Employ regular training sessions within the company to sensitise crew members about risks of weak password practices and potential consequences of unauthorised access
Office Support	Repudiation	Inside Attacker with malicious attempt targets an account that remains unattended by	Implement monitoring and auditing so system can track and log activities associated with user profile. Review and

		employee on holiday. They access crew members profile using compromised credentials or exploiting weak security measures. Once inside system, attacker alters maintenance logs and records.	analysing logs can identify unauthorised access and alterations. Employ account lockdown so that if employee is on leave or absent their account is temporarily locked or subjected to restricted access to prevent unauthorised use.
Maintenance Crew	**Repudiation**	Maintenance crew member engages with service application carrying out essential actions like modifying configurations or updating maintenance logs. Insider threat emerges as crew member attempts to manipulate or tamper with audit trails and other records so they can deny involvement. They argue that the records inaccurately depict their actions or that another individual conducted the activities	Integrate digital signatures and biometric authentication methods to tie actions directly to the responsible maintenance crew emember leaving no room for ambiguity or denial. Integration of audit logging systems that are tamper-proof. This ensures that once a record is created, it cannot be altered or deleted by anyone