Cybersecurity in the Airline Industry: A Technical Perspective

Bhanuprakash Madupati

Cision, NC

Abstract

Modern airline companies constantly rely on interconnected digital systems and networks; thus, the industry is becoming more susceptible to cybersecurity risks.This paper aims to analyze methods to improve the industry's cybersecurity by technical means with emphasis on the protection of infrastructure, data and applications. These are secure software development, endpoint protection, IDP, MFA, and encryption.Further, incorporating AI capabilities for real time threat detection and better security monitoring for new challenges in airline cybersecurity is also proposed.

Keywords: But to name a few; Airline Cybersecurity, Secure Software Development, Intrusion Detection, Endpoint Security, Multi-factor Authentication, Data Encryption, AI Cybersecurity.

1. Introduction

Aviation industry as a subsector of transportation infrastructure is experiencing tremendous growth in a way that it incorporates complex technological elements as a way of achieving efficiency and safe flying.A multitude of technologies is required within the airlines industry and these include flight management systems, air traffic control systems, as well as customer service solutions.While industry has increasingly relied on digital systems to operate its infrastructure and manage energy production and distribution, this increases vulnerability of the industry to cyber threats including data piracy, system malfunctions, advanced cyber incidents targeting the energy sector structures.

The following paper articulates that cybersecurity in the airline industry is especially noteworthy due to its multifaceted digital environment.Thus, integrating several components such as airline operational systems, reservation systems, in-flight entertainment, and ground control networks is a significant concern because it provides hackers with a large attack surface.Due to their integration and functioning as individual systems, together with the handling of valuable data such as passengers' data, flight data, and the networks through which communication is conducted, they are vulnerable to cyber threats.

Ongoing events have shown that airline organizations have many weak links in regards to cybersecurity. For example, hacking attacks on the important infrastructure dealing with airline and data leaks of passengers' data have highlighted the necessity of effective cybersecurity measures and plans.These challenges are aggravated by the regulators, for instance, the ICAO and EASA because they provide security rules necessary to protect operational and passengers' data.

The present paper is a technical analysis of the cybersecurity measures and protective solutions concerning the airlines.It includes areas of interest like secure software development, network, and end-point protection, multi-factor authentication, and encryption.Furthermore, it evaluates possible future developments, including the utilization of A.I to distinguish risky occurrences in real-time for this particular high-risk area for improvement in security measures.

Thus, it will focus on giving the reader a comprehensive view of the current state of cybersecurity in aviation and discuss how different state-of-the-art technologies and best practices can protect the vital airline systems and structures from constant evolution of cyber threats.

2.Technical Challenges and Solutions

The airline industry has specific cybersecurity risks because it is dependent on a variety of interrelated systems and networks including critical infrastructures, passengers' services, and operational facilities.The following are technical challenges/ solutions to improve security in the airline industry:

2.1 Developing Secure Software

Developing secure software systems is crucial for the aviation industry as it relies heavily on various software applications in critical systems like booking, flight management, IFE (in-flight entertainment) and communication networks. As in the digital world, these apps are subject to all kinds of security issues ranging from code injection, buffer overflow and incorrect input validation. These weaknesses could be exploited by malicious hackers to intercept unauthorized access, steal data, or disrupt the system's functioning.

For instance, code injection would prevent an attacker from inserting harmful code in an app, which could eventually result in unauthorized access or information dribbling. Moreover, buffer overflow vulnerabilities occur when an application writes more data to a buffer than it can hold, allowing attackers to overwrite critical memory with arbitrary code. Based on our experience, the problems arising from improper input validation are sizable – most are due to SQL injection, which is when attackers can manipulate a database by sending malicious queries. All of these vulnerabilities are a real threat to the lives and functioning efficiency of the air transportation industry.

Secure Software Development (SSD) practices are necessary to reduce those risks. They use static and dynamic code analysis to ensure your application has no security vulnerabilities during development. SCA involves scanning the source code of an application to identify flawed lines of codes, without running the program live. In contrast, DA is run-time testing conducted on the app, meaning developers will monitor how their software works under different conditions. These methods help identify and mitigate vulnerabilities well before they reach production, making it harder for hackers to exploit airline systems.

In a study by Gilliam et al., A Software Security Checklist is a key part of the building secure applications strategy [1]. This checklist is designed to assist in ensuring that security attributes are met during the different phases of the software development life cycle. It includes identifying vulnerabilities, regular code review, and, most importantly, continuous security testing.

Early in that design phase, developers can identify vulnerabilities and see where the software might be weak. A structured approach is taken through code reviews to analyze an application's code to verify that secure coding practices have been followed. Lastly, security testing is performed regularly during the entire software lifetime to spot vulnerabilities before they are exploited in a live system after deployment.

Applying those secure software development practices can greatly shrink the attack surface of their applications and ensure that critical systems are a tough nut to crack for cybercriminals. Given the rapid acceleration of high-tech solutions in aviation, SSDs are now more important than ever to ensure that operational systems and passenger data remain secure.**Table 1**: Software Security Checklist Across Development Phases

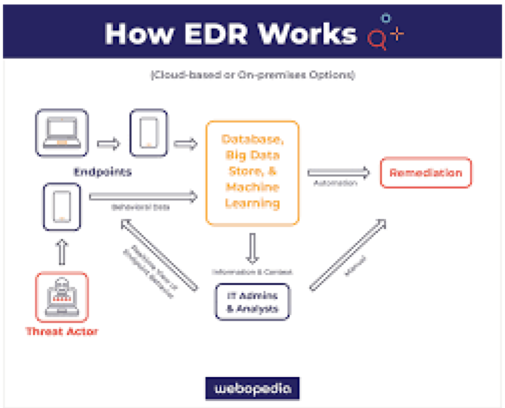
Phase	Security Measures
Design Phase	Threat modeling, Secure architecture
Coding Phase	Static code analysis, Dynamic code testing
Deployment Phase	Penetration testing, Security audits
Maintenance Phase	Patch management, Incident monitoring

2.2 Endpoint security and malware detection

With regard to the nature of an airline, it comprises a vast number of endpoints including workstations, mobile devices as well as servers that remain vulnerable and open to malware attack.Securing of these endpoints is however possible by putting in place effective security measures such as End Point Detection and Response (EDR) systems.EDR solutions intended are meant for malware mitigation in real time with a focus on endpoint activities with an additional feature of auto-response to threats.

In detail, Arfeen et al. [3] explain that EDR systems can be greatly helpful in countering malware threats in industries with crucial infrastructure.EDR solutions are used in the airline industry so that the airlines detect threats that may interfere with operations or data that contains important customer information.

Fig 1: EDR System Process

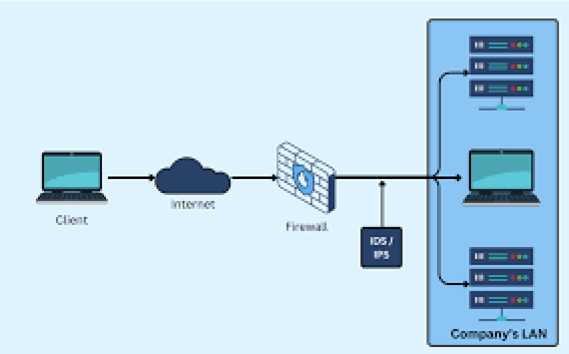


2.3 Intrusion Detection and Prevention Systems

IDS and IPS are the additional security systems that serve as the basis for the airline industry network security.IDS is mainly responsible for traffic filtering for the presence of malicious activities whereas IPS is more active as it deals with the real time filtering off the malicious traffic.IDS and IPS can be integrated into the Intrusion Management System (IMS) because the latter provides better defense by integrating the prevention with the detection.

Leng and Wang [4] discusses how IDS and IPS should becombine in order to increase real-time detection capability as well as minimize false-positive values.The IMS not only alerts the company about an anomaly, but also helps the enforcing of access control to key resources such as airline reservation databases or operation networks.It is especially advantageous for networks on an aviation scale where threats both from within and outside the network must be addressed adequately.

Figure 2: Integration of IDS and IPS in an IMS



2.4 Multi-Factor Authentication for Access Control

Security in the airline industry is highly important in order to prevent unauthorized access to data and systems in an airline including passenger details and flight schedules.The current single-factor authentication solutions like passwords have been found to be increasingly ineffective in combating modern threats including phishing and credential stuffing.Strong authentication techniques such as Multi-Factor Authentication (MFA), which makes the user identify himself by two or more methods, ensure higher security.

Ibrokhimov et al. [4] have also noted that, MFA helps to prevent unauthorized access to systems.The usage of two or more factors of authentication that is MFA should be applied in every single possible point of airline systems since a breach in one of those factors would not mean that the attackers are in control of the systems.This is particularly relevant in business contexts where systems such as air traffic control and flight scheduling services are involved.

2.5 Data Encryption for Security

Data encryption is one of the best ways to make Airbnb secure, and it is arguably also an important element in securing data for airlines. With so much sensitive data being processed on a daily basis, passenger details and payment information, as well as operational and flight data, need to be protected effectively. If compromised, this data can wreak havoc and could mean financial loss, disruption in operations, and damage to the brand. As a result, airlines must employ encryption types to protect both stored and transmitted information.

Encrypting plaintext data in a readable format is called Cleartext (or) Plain text; Encryption: changing readable data in Ciphertext. This data is, however, unreadable to unauthorized persons due to the absence of the correct decryption key. Data encryption is essential for preventing data breaches in the airline industry. Unencrypted data can be easily intercepted by cybercriminals, who use it to gain unauthorized access to valuable information. AES: The Advanced Encryption Standard (AES) is considered one of the most secure encryption protocols within the industry and is employed by airlines to encrypt sensitive data. One of the best features of AES is that it is highly secure and efficient, so when encrypting large datasets like those containing passenger records or even flight schedules, you will retain much performance from your system.

AES is based on symmetric key encryption, where a single key (a secret shared by entities that need to communicate) is used to encrypt and decrypt code. This powerful algorithm is also helpful in preventing sensitive information from being intercepted or saved by hackers during transmission. On transport, data transmissions between systems or applications use protocols like AES and Transport Layer Security (TLS) to secure this movement of information. At the same time, it is in motion so that other parties cannot view payment details and personal identification information.

Complemented by decentralized storage and blockchain advances, there is also the promise of a more secure future for airline data beyond established encryption protocols. As mentioned by Alessi et al. Using decentralized storage with blockchain for encrypted distribution[7] Even if a server is breached through external, especially if internal, like insider threats, data integrity is increased — and your access to unencrypted backup will still be safe. If an attacker were to compromise some part of the blockchain, he would only be able to see shattered parts of data, not the complete dataset.

They are adding security to the airline industry, including decentralized data storage in-flight and encryption. This means that important operational and passenger data is more secure from external attacks and internal threats. The airline also encrypts the data before storing it across the blockchain, reducing its exposure to hacking or data leakage even if multiple systems or employees share information.

Encryption can also be an important component of compliance. Numerous nations have quite authoritarian laws regarding data protection (Europe, specifically the General Data Protection Regulation or GDPR). Airlines can avoid fines and enforce customer trust by following these regulations, such as using strong encryption techniques to encrypt data.

As a result, encryption — whether via well-known protocols like AES and TLS or newer companies such as blockchain — continues to be an essential weapon in the cybersecurity armory of today.— The airline industry relies upon encryption too. In order to respond accordingly to the evolving cyber threats, the implementation of encryption will also need to adapt to mitigate them and ensure that sensitive operational and passenger data is always safe.**Table 2**: "Common Encryption Protocols for Data Protection"

Encryption Protocol	Use Case
AES	Data at rest and in transit
TLS	Secure communication in networks
RSA	Secure key exchange

3.Discussion

3.1. Secure Software Development

In the airline industry, this is why it is important to ensure that only secure software systems are developed so as to ensure that security breaches do not occur and compromise sensitive information and operations.Adoption of a Software Security Checklist for the software development life cycle is also another robust safety measure that minimizes risks that are likely to be known towards the end of the development process.Gilliam et al. [1] stated that implementing security measures right from the start minimizes the threat of prevalent issues including code injection or insecure configurations.Due to the fact that the airlines system are extensive with various intricate connections, this preventive approach can be critical in reducing the attack surface.

Again, the aspects of SSP are equally useful in shielding the interfaces between the various systems.For instance, many operational applications require accurate exchange of data, such as airline reservation systems, operation databases, and communication networks.This meant that any vulnerability in one system could mean the whole network is at risk of cyber threats.Therefore, through the implementation of security at each stage of development, the airline’s systems can be protected against a number of different threats.

3.2 Enhancing Endpoint Security

Airlines need to protect numerous endpoints that is used in daily operations, such as, employees’ devices, operational workstations, and significant servers.Endpoint Detection and Response systems presents very effective solution for endpoint threats real-time detection and response.Citing Arfeen et al [3], EDR systems ensure that potential and active threats are detected in advance, enabling their containment and elimination before they go viral.In the context of airlines, this capability is critical as an attacker might get control of a specific endpoint, and thus gain access to important organizational systems including flight control as well as passenger information databases.

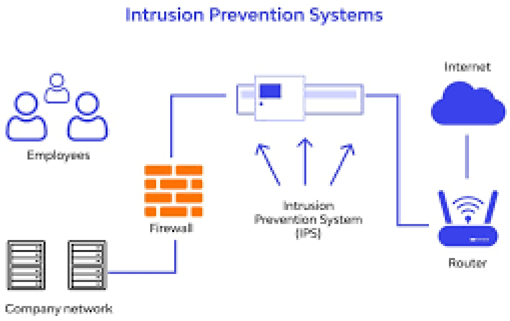
Implementing EDR solutions on all active endpoints ensures that the environment has a strong protection against malware, ransomware, and other endpoint-based threats.It is more relevant for geographically dispersed airline operations because devices located in various areas can become a target of interest for a searching for vulnerabilities in entry points.

3.3 The Intrusion Detection and Prevention Systems

The implementation and execution of IDS and IPS through an IMS presents a detailed solution for safeguarding airline networks.The key benefit of the integration of IDS and IPS is that while IDS only passively scouts network traffic for different types of suspicious actions and continuously reports on its findings, IPS actively shields against unauthorized login attempts in real time.

Leng and Wang [5] have pointed out that the integration of IDS and IPS in an IMS not only increases the level of security but also minimizes the chances of false positives that may compromise operations.This is quite relevant to airline networks, where even slight disturbances can lead to operational setbacks or even compromise safety.Moreover, the ability to block proactively of the IPS is invaluable to protect from new, potential threats, such as zero-day vulnerabilities, which could harm critical infrastructure if left unmitigated.

Fig: Intrusion Prevention System

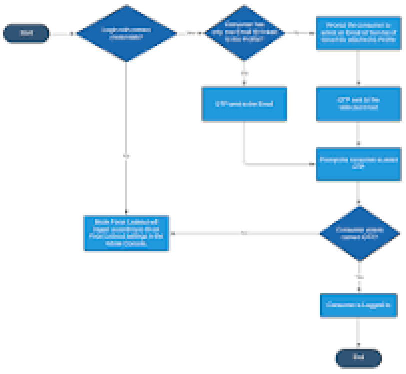

Intrusion Prevention Systems
Employees
Internet
Firewall
Intrusion Prevention System (IPS)
Router
Company network

3.4 Multi-Factor Authentication for Critical Systems

The adoption of Multi-Factor Authentication (MFA) remains one of the primary proactive steps in protecting airline systems from unauthorized access.Since credential theft and phishing are becoming rampant, relying on passwords alone is not secure enough.MFA provides the user with multiple types of identities such as password and smart finger touch or one-time number that enhances security.

Ibrokhimov et al. [4] pointed out that MFA tissues are highly useful in the domains of cyber-physical systems; the extra factors of identification significantly decrease the chances of hacking even if one factor is shared.This is well applicable in the airline business to safeguard several critical applications that if penetrated by hackers may lead to disastrous outcomes including the flight schedules, the traffic control systems, and maintenance programs.

Fig 3: MFA Process Flowchart

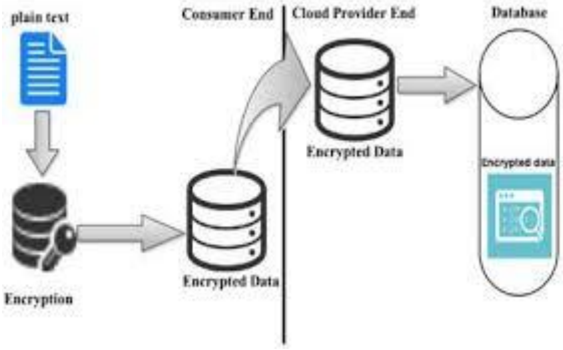


3.5 Data Encryption for Protecting Sensitive Information

The safeguarding of passenger details and other organizational data through encryption is another significant aspect of cybersecurity.Data encryption makes it impossible for the attackers who may have compromised a particular system to access information that they have no decryption authority.AES is among the widely applied algorithms for data encryption in the airline industry to ensure that data is protected when finally stored and when in transit.

Alessi et al. [7] have noted that deploying encryption along with distributed storage like blockchain improves the data privacy by distributing data across the nodes.This approach reduces the exposure of a given breach whereby an attacker would have to penetrate through the different layers in order to get the entire set.For airlines, this means that information such as passenger's payments details, flight logbooks, and communications can be encrypted and well protected from the network access in case of a breach.

Fig 4: Data Encryption Process Diagram



3.6 The Future Use of Artificial Intelligence in Cyber Security

AI can also be adopted as a tool to defend the airline technology from new threats as it offers bespoke solutions in real-time.AI-based systems can consider extensive data acquired from the network and identify the signs of a cyberattack far faster and more effectively than conventional approaches.

AI can also be implemented for cross protocol interactions of various IoT devices which are incorporated into the airline operation such as smart airport and connected aircraft system as described by Ge et al. [6].When airlines have implemented AI cybersecurity solutions, activities on the network can be observed and potential threats can also be detected in real time.

4. Conclusion

Secure Software Development:

Using proposed security features during the software development life cycle including code review and vulnerability assessment significantly reduces vulnerabilities in airline systems [1].

Endpoint Security:

The Endpoint Detection and Response (EDR) technology is useful for the protection of workstations, mobile devices, and servers, being a real-time protection against malware and ransomware in the airline industry [3].

Intrusion Detection and Prevention:

Connecting the IDS with the IPS through an IMS forms a layered defense system that enhances airline defenses by including more proactive IDS/IPS [5].

Multi-Factor Authentication (MFA):

It is important to apply MFA to all crucial systems in the airline industry, mainly in the flight schedule, air traffic control, and maintenance [4].

Data Encryption:

Securing data whether stored or in transit means that even if the systems are compromised, the data will still not be easily vulnerable to unauthorized use.Other advantages of decentralized storages are [7]:

Artificial Intelligence in Cybersecurity:

Cybersecurity solutions that incorporate AI are far more effective in real-time protection with first response mechanisms and adaptability in monitoring IoT devices and core airline assets [6].

References

1. D. P. Gilliam, T. L. Wolfe, J. S. Sherif, and M. Bishop, “Software security checklist for the software life cycle,” IEEE Xplore, Jun. 01, 2003. doi: https://doi.org/10.1109/ENABL.2003.1231415. Available: https://ieeexplore.ieee.org/abstract/document/1231415.
2. A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, “Endpoint Detection & Response: A Malware Identification Solution,” 2021 International Conference on Cyber Warfare and Security (ICCWS), pp. 1–8, Nov. 2021, doi: https://doi.org/10.1109/iccws53234.2021.9703010.

3. L. Leng and L. Wang, “The fusion method of the IDS and IPS based on IMS,” IEEE Xplore, Aug. 01, 2012. doi: https://doi.org/10.1109/CSIP.2012.6308956. Available: https://ieeexplore.ieee.org/document/6308956.
4. S. Ibrokhimov, K. L. Hui, A. A. Al-Absi, H. J. Lee, and M. Sain, “Multi-Factor Authentication in Cyber Physical System: A State of Art Survey,” IEEE Xplore, Feb. 01, 2019. doi: https://doi.org/10.23919/ICACT.2019.8701960. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8701960.
5. M. Alessi, A. Camillo, and M. Matera, “Make Users Own Their Data: A Decentralized Personal Data Store Prototype Based on Ethereum and IPFS,” IEEE Xplore, 2018. Available: https://ieeexplore.ieee.org/document/8448350.
6. M. Ge, J. B. Hong, H. Alzaid, and D. S. Kim, “Security Modeling and Analysis of Cross-Protocol IoT Devices,” 2017 IEEE Trustcom/BigDataSE/ICESS, Aug. 2017, doi: https://doi.org/10.1109/trustcom/bigdatase/icess.2017.350.
7. M. Sodanil, G. Quirchmayr, N. Porrawatpreyakorn, and A. M. Tjoa, “A knowledge transfer framework for secure coding practices,” IEEE Xplore, Jul. 01, 2015. doi: https://doi.org/10.1109/JCSSE.2015.7219782. Available: https://ieeexplore.ieee.org/abstract/document/7219782.