Advances in Networks
2022; 10(1): 7-14
http://www.sciencepublishinggroup.com/j/net
doi: 10.11648/j.net.20221001.12
ISSN: 2326-9766 (Print); ISSN: 2326-9782 (Online)

Hacking an Aircraft: Hacking the In-flight Entertainment System

Eman Ali Metwally[*], **Haytham Tarek Mohammed**

Faculty of Computers and Information Science, Mansoura University, Mansoura, Egypt

Email address:
eman.ali.metwally@gmail.com (E. A. Metwally)
[*]Corresponding author

To cite this article:
Eman Ali Metwally, Haytham Tarek Mohammed. Hacking an Aircraft: Hacking the In-flight Entertainment System. *Advances in Networks*. Vol. 10, No. 1, 2022, pp. 7-14. doi: 10.11648/j.net.20221001.12

Received: May 9, 2022; **Accepted**: May 30, 2022; **Published**: June 14, 2022

Abstract: When it comes to systems that rely on computers and communications, we describe security as the prevention of intentional and, to a large extent, unintentional misuse that could compromise desired system behavior. In the context of existing safety, development, and certification, this study provides a practical understanding of how cyber security effects airplane computer system architecture. There's more to aviation than planes. It is backed up by the necessary ground infrastructure and equipment, as well as a large-scale computer network. Operations using computer networks to disrupt, deny, degrade, or destroy information housed in computers and computer networks, or the machines and networks themselves, are known as virtual attacks against the computer network. This paper discusses some of the most important security concerns that occur when it comes to aviation safety and reliability. We believe that many of the past accidents may have been perpetrated deliberately, and that some of them could be replicated maliciously now. We begin by looking at common security weaknesses and threats in aviation and its supporting infrastructure, as well as recalling some prior occurrences. Then we analyze what catastrophes are probable, if not inevitable, and what we might do in response.

Keywords: Aviation, Information Security, Cyber Attack

1. Introduction:"Welcome Aboard This Is Your Hacker Speaking"

Cyber-attacks and cyber security are in the world news every day. Systems controlled by embedded computers (Cyber-Physical System or CPS) are increasingly featured as being at risk, with concern continually expressed over the vulnerability of critical infrastructure to damage and disruption from attacks over networks. Digital control systems in aircraft are also CPS and are likewise the subject of concern. Both Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) have created regulations to address such concerns, and RTCA and EUROCAE have published process guidance. This guidance is expected to ultimately establish standards of practice for regulators and the industry to develop and certify aircraft for which network security is a requirement. However, the implications to project costs and schedules, designs, and the practical aspects of implementation remain largely unknown to aircraft system designers. This paper provides a practical understanding of how cyber security impacts airplane computer system design, in the presence of existing safety, development, and certification requirements and processes, 2012 by The Boeing Company [1].

Aviation is more than just planes. It is supported by the needed ground equipment and systems as well as large scale computer network. Virtual attack against the computer network consists of operations using computer networks to disrupt, deny, degrade, or destroy information residing in computers and computer networks or the computers and networks themselves. Private companies working within the internet security industry report a growing level of hacking aimed at key industries and aviation industry is, without a doubt, one of them. Many hackers or terrorist groups may consider cyber-attacks as an easy, cheap, and very effective mean of demonstration of strength. Every radar, every air traffic controller/Air traffic management (ATC/ATM) system, every link, and every phone line that makes the system a potential target. Cyber-attacks have become a global pandemic and no system is immune. The hackers could remove e.g., all the protections of a traffic collision avoidance system which can lead to mid-air collision and consequent misuse of sensitive data is something that really needs to be addressed [2].

The civil aviation sector in the world has become exposed to many risks, foremost of which are cyber security threats, and the fear of penetration of aircraft systems, as aircraft include a complex network of components, communication links and sensors, which are vulnerable to electronic attacks, whether hacking or jamming, and therefore, Cyber-attacks can cripple civil aviation, including hacking flight electronic systems, interfering with radar and communications systems, and disrupting multiple systems at airports.

Several international experts in the field of aviation confirmed that hackers can penetrate the electronic systems of civil aircraft even while they are in the air. Therefore, the importance of precautionary measures comes considering the technological nature of civil aviation, as well as its role in the global economy. In this article, we present a vulnerability assessment framework that could be used to assess and prevent cyber threats related to wired and wireless networks and computer systems in planes. We have performed vulnerability overview for aviation systems to meet aviation industry requirements for wireless network security. This paper contributes to improve security and safety of aircraft via the corresponding recommendations.

2. Hacking Steps

The penetration of the information system takes place in four stages as shown in figure 1.

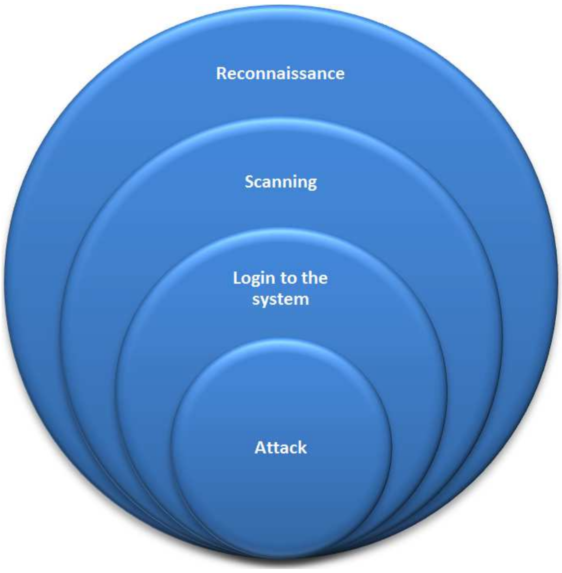

Figure 1. *four stages for penetrating the information system.*

Scanning: In this stage, the hacker uses the information collected in the survey stage to gather more details related to the victim's network such as the active hosts on the network, open ports, IP addresses, system architecture, services, and vulnerabilities for all the parts that are being scanned.

Login to the system: The hacker uses the information and ciphers to enter the target operating system.

Attack: in which the hacker takes control of the system and carry out the required task.

Reconnaissance and fingerprint detection: This stage is a preparatory stage for system penetration, as it includes gathering as much information as possible about the target including the network used, operating systems, applications, web server version and system-related vulnerabilities.

2.1. Does the Hacker Have a positive Role

Actually, the positive role is the one of the security penetration testers who checks over the system in a legal and good way for:

1) Detecting security flaws and filling gaps.
2) Developing and modifying programs on the Internet.
3) Providing security consultancy for huge companies such as Microsoft, Google, and others, as well as airlines and industrial institutions and archiving government information.
4) Assisting the security authorities, preventing the entry of intruders, and filling the gaps to control those who abuse the system.
5) Providing security advice to major companies such as Microsoft, aircraft building companies, and major industrial institutions, as well as government information archives, to prevent theft of device and machine designs by competitors at the national or international level, and to prevent abusers from entering their networks that contain confidential or sensitive issues and prevent vandalism.

2.2. Threats in the Security of Aviation Cyber-Physical Systems

Onboard sensor and actuator networks in aviation systems and connected aircraft have both wired and wireless nodes that monitor and manage the interior and exterior surroundings of aircraft, as well as onboard physical components and assets. As a result, vulnerability assessments and penetration tests must be performed on wired and wireless nodes and networks, including (1) cabin services systems, crew devices, airline information services, passenger information, entertainment services, and maintenance systems, and (2) wireless data links (based on IEEE 802.11 and IEEE 802.16 technologies) and (3) Air Traffic Control and Satellite communications, and Airline Info Services Domains [3].

As shown in figure 2, the following are some of the main threats in the Security of Aviation Cyber-Physical Systems Network due to Wi-Fi 802.11 wireless network related assaults, where due diligence is essential [4].

1) *Data Interception:* It is well understood and agreed that data sent over Wi-Fi can be easily intercepted by eavesdroppers within a few hundred feet; even further with directional antennae. Unfortunately, many WLANs are set up to handle both the Advanced Encryption System (AES) and the Temporary Key Integrity Protocol (TKIP), and legacy products only support TKIP. TKIP, on the other hand, is vulnerable to message integrity check (MIC) attacks, which allow only a small number of forged frames into a protocol. [5].

2) *Denial of Service (DOS attack):* Denial-of-service attacks are naturally possible on WLANs. Due to the fact that air traffic uses the same unlicensed frequencies, there is unavoidable competition in heavily populated areas. WLANs will be able to use channels in the 5 GHz band, which are larger and less crowded, as they migrate to 802.11n, reducing "accidental DoS." Modern access points can also adjust channels automatically to avoid interference. However, there are still several DoS attacks to take into account: Phony messages are sent to disconnect users, consume AP resources, and keep channels operational. To mitigate popular DoS attack methods, newer systems that enable 802.11w management frame security are required (Deauth Flood, Deauthentication DOS aattack, etc.) [6].
3) *Rogue Access Points:* Penetration of the aviation network by unknown, unauthorised APs is a major security concern. Unfortunately, tracing the wired network connectivity of "real rogues" is a talent that conventional WLAN hardware has yet to master. Automated rogue blocking is a dangerous endeavour without good classification. Implement a Wireless Intrusion Prevention System (WIPS) that can reliably distinguish between innocent neighbours, personal hotspots, and network-connected rogues that constitute a serious threat, and take policy-based action to trace, block, and locate the latter to efficiently detect and neutralise rogue APs.
4) *Wireless Intruders:* Malicious Wi-Fi clients operating in or near a business' airspace can be detected with WIPS devices such as Motorola AirDefense, AirMagnet, and AirTight. However, genuinely effective defense against wireless invaders necessitates the use of up-to-date, correctly deployed WIPS sensors. 802.11a/b/g sensors, in particular, need to be updated to monitor new 5 GHz channels (including 40 MHz channels), parse 802.11n protocols, and detect new 802.11n assaults. Additionally, because 802.11n clients can connect from a greater distance, WIPS sensor location must be revised to meet both detection and prevention requirements.
5) *Misconfigured Access Points:* Configuration failures posed a substantial security issue when isolated APs were individually handled. However, 802.11n introduces a deluge of somewhat complex configuration choices, the effects of which are greatly dependent on the capabilities of Wi-Fi clients. Configuration is further complicated by multi-media prioritization and division.
6) *Ad Hoc and Soft APs:* Risky peer-to-peer ad hoc connections that bypass network security safeguards have long been possible with Wi-Fi laptops. Unfortunately, this barrier is being removed by "soft APs" in new mobile devices with Intel and Atheros Wi-Fi cards. These virtual APs can provide customers with simple, automatic direct connections, bypassing network security and relaying traffic onto the enterprise network. IT-managed client settings and WIPS, which are used to prevent illicit Ad Hoc connections, may also be useful against unauthorized Soft Aps. [7, 8].

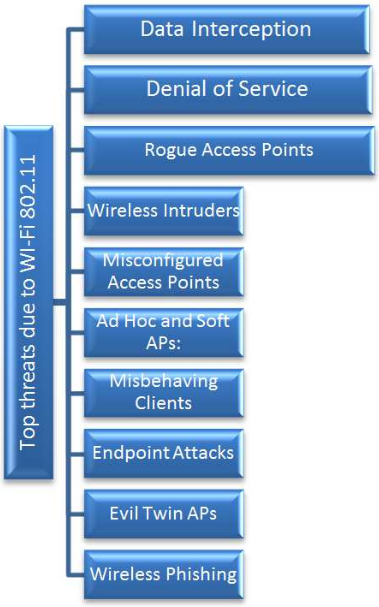

Figure 2. *Threats in Wi-Fi 802.11 wireless network related attacks in Security of Aviation Cyber-Physical Systems network.*

7) *Misbehaving Clients:* Clients who create unauthorized Wi-Fi connections of any kind, whether unintentionally or on purpose, jeopardies themselves and their company's data. Certain businesses utilize Group Policy Objects to configure allowed Wi-Fi connections and block end-user changes. Others use host-resident agents and/or WIPS to monitor Wi-Fi client activities and disconnect high-risk connections. End-users are still expected to connect only to recognized, authorized wireless access points in many organizations. Because of ACPS's extensive deployment, greater reach, and broader consumer electronics integration, making accidental or unauthorized Wi-Fi connections has never been easier. As a result, it's vital to act quickly to prevent Wi-Fi client misbehavior.
8) *Endpoint Attacks:* Now that over-the-air encryption and network-edge security have improved, attackers are refocusing their efforts on Wi-Fi endpoints. Several exploits have been discovered that take advantage of faulty Wi-Fi drivers and leverage buffer overflows to execute arbitrary commands. Automated attack tools like Metasploit can now launch Wi-Fi endpoint exploits with minimal effort.
9) *Evil Twin APs:* Fraudulent APs can readily advertise the same network name (SSID) as a real hotspot or enterprise WLAN, causing nearby Wi-Fi clients to join to them. Although evil twins aren't new, the popularity of easier-to-use hacking tools has increased the likelihood of coming across one. Tools like Karmetasploit may now listen in on neighbouring clients to determine which SSIDs they're willing to

connect to, and then automatically advertise those SSIDs.

10) *Wireless Phishing:* Hackers continue to explore new methods to phish Wi-Fi users in addition to the above man-in-the-middle application assaults. Poisoning Wi-Fi client Web browser caches, for example, is possible if the attacker can break into a previous Web session, such as by using an Evil Twin at an open hotspot. Vulnerability assessments and penetration tests can help aviation and space system businesses, such as commercial aircraft builders and other commercial airlines, improve their cyber security efforts. [9, 6, 10].

3. Cyber-Attacks Incidents in the Civil Aviation Industry

The following table 1 provides reviews of documented cyber-threats and assaults in the civil aviation industry during the previous 18 years in this context, in which C = Confidentiality, I = Integrity, A = Availability. Although some cyber-attacks in the civil aviation business during the period under consideration may have been missed because some occurrences were not made public. Incidents from the Online Technical Report and News.

3.1. Real Attack Scenario

3.1.1. Chris Roberts

Security expert hacking into a commercial airliner and making it fly aside' bragging that he also hacked the International Space Station as Chris Roberts told an audience at GrrCON 2012 hacker conference how he managed to alter the temperature aboard the ISS spaceship eight or nine years ago in a video that was... Newly disclosed from the event, Roberts says he "had problems" with NASA, but hacking the communication controls was "absolutely fun". "If they're leaving the site open and unencrypted, it's their silly mistake," he also said, as Roberts told an FBI agent earlier this year that he had hacked into the In-flight entertainment (IFE) system systems of commercial planes.

While his laptop and tablet were confiscated for further investigations and held for investigation for several hours, the airline canceled his return ticket. Later during investigations, Roberts admitted that he could control the aircraft's management systems for a specified time and that he was even able to change the plane's direction. In addition, he revealed the details of the hacking operation, infiltrating the aircraft's IFE systems by connecting to it with a specially prepared software [31].

3.1.2. An Airbus A330 Crashed in the South Atlantic, Missing 228 People

The computers in the aircraft's control system are programmed to identify if data being sent to them is anomalous, and if so, to shut down so that pilots can manually fly the plane. The flight management system for Air France Flight 447 from Rio to Paris, for example, was shut down in 2009 due to false data from an instrument that had failed due to icing.

Manual control of the crew should have been possible. They never regained control due to poor training, and an Airbus A330 crashed in the South Atlantic, killing 228 people. All pilots have gotten new training since then to ensure that they can recover when computers fail. However, no team has yet had to deal with the implications of an intruder hacking its flight protections. [32]

3.2. Loopholes and Breach Points on Aircraft

In addition to USB, some aircraft have RJ-45 ports that allow even greater hacking attempts on a connected laptop. A professional hacker may be able to take control of the aircraft's multimedia system and control the server as well, which is a difficult but feasible challenge.

The main issue is that some aircraft have additional RJ-45 ports described as “private use only,” and it is possible that when connected to this port, a hacker could gain access to sensitive system elements. On the other hand, there are cases of manufacturing defects because of gaps in the program, as recently 3 out of 4 Airbus engines failed during takeoff due to data loss because of a wrong update in the program, which led to the crash of the plane [33].

USB and communications services play a big and dangerous role, as the device that provides internet service to the passenger is the same that provides internet service for navigation and guidance devices, which in turn may allow the hacker to access the control panel of the plane.

3.2.1. Can a Plane Be Hacked via Its Entertainment System

1) Technically, the hacker may be able to use the USB port to connect a flash carrying a system or hacking program, and through the screen in front of him in the IFE - which companies usually put in the back of the seat in front of you as a kind of entertainment factor - he restarts the device by booting through the flash on which the harmful system is loaded.
2) With this step, the hacker was already able to control the IFE for the passenger seat on the plane.
3) And then, with great ease, he can control the displays on the plane which provides information on altitude - atmospheric pressure and flight path. And from here it can do many things, like cause panic on the plane - providing false information about the flight path, landing place, arrival time or displayed on screens for passengers. It can also control what passengers see on their screens.
4) The hacking system that was developed via USB can analyze security vulnerabilities in higher systems.
5) At this stage, the hacker tries to take control of the ISP device on the plane, which is moderately protected by exploiting security holes or vulnerabilities to penetrate the ISP.
6) Hence, he will not be able to monitor and analyze everything that passengers do over the Internet in addition to eavesdropping on passengers' calls, and the most dangerous is that he can change and control the

information provided by the Internet provider device to the flight management system.

7) From here, the hacker begins to provide wrong information to the Flight management system about altitude coordinates, atmospheric pressure, weather conditions, and more seriously, he can change the flight path at this point.
8) At this stage, the hacker can disconnect the Internet from the Flight Management System, which deprives the plane of the instantaneous information that it has, and it cannot also provide distress on the Internet.

3.2.2. GPS

Civilian GPS signals are designed as an open standard, freely accessible to all. These virtues have made civilian GPS incredibly popular, but the transparency and predictability of its signals lead to danger: they can easily be falsified or spoofed. Civilian GPS signals have a detailed structure but no built-in anti-counterfeiting protection. Civil GPS is the most unsecured protocol in the world [34].

3.2.3. Ethernet

1) The hacker can exploit the “Ethernet” located under his seat on the plane to connect it to the laptop computer loaded with Hacking System, through which he can find the Vulnerabilities on the different systems on the plane, noting that all the systems on the plane “entertainment - lighting - displays - electricity and fuel - Flight Management System - the cockpit - and the main server on the plane, by trying to hack the following, starting with espionage - Sniffing Attack - Man in the middle attack - and hacking the Internet protocols, and then it can spy on what users are doing in real time.
2) The hacking system that was developed by the laptop can analyze security vulnerabilities in higher systems.
3) At this stage, the hacker tries to control the plane's internet service provider by exploiting security holes or vulnerabilities to penetrate it.
4) From here, he will not only be able to monitor and analyze everything that passengers do over the Internet and can eavesdrop on passengers' calls, and the most dangerous thing is that he can change and control the information provided by the Internet provider device to the flight management system, and from here the hacker begins to change the coordinates of altitude, air pressure and status The weather and the most dangerous thing is that the hacker at this stage can cut off the Internet connection from the Flight Management System, which deprives the plane of the instantaneous information that it has, and it cannot even provide distress via the Internet.
5) And he can now launch what is known as Man in the middle attack, which enables him to penetrate the Certificate, which is the highest protection system in the plane, such as the flight control system or the engine control system, or at least partial control or control of one of the engines, as Chris Robert did the lighting, or the Air Conditioners can also be controlled.
6) If the hacker can do all the previous steps, he can penetrate the main server of the plane and thus have full control and ownership of the plane.

3.2.4. Data Communications Between the Aircraft and Ground Stations (ACARS)

To meet the security standards for wireless networks in the aviation sector. Using penetration testing tools like Metasploit Pro and Backtrack, we can uncover internet vulnerabilities in aviation systems and improve aircraft security and safety. The results of the tests on cyber vulnerabilities will be used to design effective remedies to address these flaws. New vulnerability assessments will be carried out until the solutions are deemed safe to employ. [35]

(i). The Role of IFALPA

The International Federation of Pilots Association IFALPA issued a working paper, 2021, to counter electronic attacks on aircraft and sensitive infrastructure, including the need to strengthen the security of computer hardware and software, data protection, physical separation between sensitive systems, and training of aircraft crews and Working with other international organizations and aviation stakeholders towards the development and implementation of Aviation Security Programs [36].

(ii). The Role of the International Civil Aviation Organization

The organization held the International Civil Aviation Organization "ICAO" Cyber Security Summit, in Dubai in April 2017, with the attendance of more than 80 countries. The summit set a set of goals that it sought to achieve, represented in enhancing understanding of the risks and threats posed by aviation security breaches to systems and data civil aviation, and to encourage cooperation and exchange of information and experiences between countries [37].

4. Recommendations

Technological recommendations to address cyber security threats:

1) Separating the networks for passenger’s entertainment from the network for controlling and controlling the aircraft, where two completely separate networks are implemented from each other, especially the Flight Management Guidance Computer (FMGC) device.
2) Ensure that the IFE system is turned off during landing and take-off.
3) Renewing the protection of aircraft programs through encryption so that they do not respond easily to hacking attempts.
4) Continuous updating of aircraft device drivers.
5) Establishing monitoring networks and continuous analysis of data from and to all devices on board the aircraft. In the event of any change in the sequence of entering commands to the control systems on the aircraft, the source is immediately identified to ensure its identity and is separated from the aircraft system before full control of the aircraft is achieved.
6) A tablet is available for each seat on the plane, and its

operating system is very limited for entertainment purposes only.

7) Training the pilots on manual driving to avoid danger when there is an electronic intervention.
8) Use a network-integrated device such as a Cisco 9000 or higher version with support for Virtual DDoS protection, analyze system response metrics (such as Stateful Packet Inspection (SPI) based on OpenFlow Application Centric Infrastructure (OACI) for securing critical network- SPI-OACI delay, throughput, and consumption), and provide a practical proposal to secure similar project management systems running in the cloud against cyber terrorists.
9) Recognize radio frequency jamming or electromagnetic pulse attacks as a severe hazard to air transportation and seek a solution. (We will propose a solution in our future effort.)

Table 1. *Documented cyber-threats and assaults in the civil aviation industry.*

Security breach	**source**	**year**	**Incident**	**Place**	**Description**
C	[11]	2003	Slammer Worm attack	USA	A slammer worm attack corrupted one of the FAA's administration servers. As a result of the attack, internet services were shut down in several parts of Asia, slowing connectivity around the world.
A	[12]	2006	Cyber-Attack	Alaska, USA	Two distinct cyberattacks led the US FAA to shut down portions of its air traffic control systems.
C	[12]	2008	Malicious hacking attack	Oklahoma, USA	When hackers gained control of the FAA's interconnected networks, they obtained the administrative password. They were able to acquire access to more than 40,000 login credentials used to manage part of the FAA's mission-support network by gaining access to the domain controller in the Western Pacific area.
C	[13]	2009	Malicious hacking attack	USA	Hackers obtained access to personal information through a hostile hacking assault on the FAA's computer.
C	[14]	2013	Malware attack	Istanbul, Turkey	Due to a malware attack, the passport control systems at Istanbul Ataturk and Sabiha Gokcen airports were shut down, causing several flights to be delayed.
C	[15]	2013	Hacking and phishing attacks	USA	Around 75 airports were targeted by malicious hacking and phishing activities. An unidentified nation-state is suspected of carrying out these significant cyber-attacks in order to access US commercial aviation networks.
A	[16]	2015	DDoS attack	Poland	A cyber-criminal launched a Distributed Denial-of-Service (DDoS) attack against LOT Polish Airlines' flight-plan IT Network systems at Warsaw Chopin Airport. The attack rendered LOT's system computers unable to relay flight plans to the aircraft, resulting in the cancellation of at least 10 flights and the stranding of around 1400 passengers.
I	[17]	2016	Hacking, phishing attacks	Vietnam	Pro-Beijing hackers defaced a website belonging to Vietnam Airlines, as well as flight information screens in Ho Chi Minh City and Hanoi, displaying slogans in support of China's maritime claims in the South China Sea.
A	[18]	2016	Cyber-attack	Boryspil, Ukraine	A malware attack was discovered on a computer in Kyiv's main airport's IT network, which includes the air traffic control system.
A	[17]	2017	Human error	United Kingdom	A contracted engineer disconnected and reconnected the data center power supply, causing a computer system breakdown on a British flag-carrier. Around 75,000 British Airways customers were stuck as a result of the disaster.
C	[19]	2018	Data breach	Hong Kong	Cathay Pacific Airways suffered a data breach that exposed the personal information of around 9.4 million customers.
C	[20]	2018	Data breach	United Kingdom	British Airways had a data breach that exposed the personal information of around 380,000 customers.
C	[21]	2018	Data breach	USA	Through a third party, Delta Air Lines Inc. and Sears Departmental Stores reported a data compromise of around 100,000 consumers' payment information.
A	[22]	2018	Ransomware attack	Bristol Airport, UK	At Bristol Airport, there was an attack on electronic flight information screens. As a result, the screen was turned off and replaced with information from a whiteboard. This attack has no known negative consequences.
C	[23]	2018	Mobile app data breach	Air Canada, Canada	A data breach at Air Canada's mobile app affected 20,000 people's personal information.
C	[24]	2018	Ransomware attack	Chicago, USA	The WannaCry computer virus infected Boeing, but the attack only caused minor damage to the company's internal systems.
C	[25]	2019	Cyber-Incident	Toulouse, France	Unauthorized access to Airbus' "Commercial Aircraft business" information systems because of a cyber incident. According to the report, there was no known impact on Airbus' commercial operations.
C	[26]	2019	Ransomware attack	Albany, USA	The Albany International Airport was the target of a ransomware assault over the holidays in 2019. The attackers were able to encrypt the airport's complete database, forcing the authorities to pay a ransom in exchange for the decryption key from a threat actor.
C	[27]	2019	Phishing attack	New Zealand	Customers of Air New Zealand Air-points were the victim of a phishing campaign. This hack exposed the personal information of about 112,000 clients, including names, addresses, and Air points numbers.
C	[28]	2020	Ransomware attack	Denver, USA	A cyber-attack in which the attacker gained access to and stole company data, which was then disclosed online.
C	[29]	2020	Ransomware attack	San Antonio, USA	ST Engineering's aerospace business in the United States suffered a data breach, which was followed by a ransomware attack by Maze Cyber-criminals.

Security breach	source	year	Incident	Place	Description
I	[30]	2021	Software Error	Birmingham, United Kingdom	The aircraft had 1606 kg more take-off mass than required due to a software fault in the IT system that failed to recognize mass discrepancies between the load sheet and the flight plan.

5. Conclusion

There's a lot more to aviation than planes. It is backed up by the necessary ground infrastructure and equipment, as well as a large-scale computer network. Operations using computer networks to disrupt, deny, degrade, or destroy information housed in computers and computer networks, or the machines and networks themselves, are known as virtual attacks against the computer network. Future researchers can dig more in the previously discussed points in order to find more relative results and suggestions that can be taken into consideration within the aircrafting technology.

Abbreviations

(Cyber-Physical System or CPS), Federal Aviation Administration (FAA), air traffic controller/Air traffic management (ATC/ATM) system, Wireless Intrusion Prevention System (WIPS), Flight Management Guidance Computer (FMGC), In-flight entertainment (IFE) system, Stateful Packet Inspection (SPI).

Acknowledgements

I would like to express my special thanks of gratitude to *Mr. Mohammed Shaker* who pushes me towards the golden opportunity to publish this article, as any attempt at any level could not have been completed without his unwavering support and guidance. I am grateful to him for enlightening the idea at the first glance.

Mr. Mohammed, "Your support made this work possible".

References

[1] C. Royalty, "Cyber Security for Aeronautical Networked Platforms - What does it mean to me in commercial aviation design?," 2012, doi: 10.2514/6.2012-2417.

[2] S. Tomáš, K. Ivan, and S. Stanislav, "Present and potential security threats posed to civil aviation," *Incas Bull.*, vol. 4, no. 2, pp. 169–175, 2012, doi: 10.13111/2066-8201.2012.4.2.17.

[3] M. L. Olive, R. T. Oishi, and S. Arentz, "Commercial aircraft information security-an overview of ARINC report 811," *AIAA/IEEE Digit. Avion. Syst. Conf. - Proc.*, pp. 1–12, 2006, doi: 10.1109/DASC.2006.313761.

[4] C. A. Wargo and C. Dhas, "Security consideratiolis for the e-enabled aircraft," *IEEE Aerosp. Conf. Proc.*, vol. 4, pp. 1533–1550, 2003, doi: 10.1109/AERO.2003.1235083.

[5] N. Thanthry and R. Pendse, "Aviation data networks: Security issues and network architecture," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 20, no. 6, pp. 3–8, 2005, doi: 10.1109/MAES.2005.1453803.

[6] R. Robinson, M. Li, and K. Sampigethaya, "Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety ƒ A irplane A ssets D istribution S ystem ƒ Assessment according to the Common Criteria ƒ Conclusion," no. September, pp. 1–18, 2007.

[7] S. K. P. Alampalayam and S. Srinivasan, "Intrusion Recovery Framework for Tactical Mobile Ad hoc Networks Intrusion Recovery Framework for Tactical Mobile Ad hoc Networks," no. May, 2014.

[8] S. A. Kumar, "Classification and Review of Security Schemes in Mobile Computing," *Wirel. Sens. Netw.*, vol. 02, no. 06, pp. 419–440, 2010, doi: 10.4236/wsn.2010.26054.

[9] S. a Lintelman, K. Sampigethaya, M. Li, R. Poovendran, and R. V Robinson, "High Assurance Aerospace CPS & Implications for the Automotive Industry," *Proc. Natl. Work. High Confid. Automotice Cyber-Physical Syst.*, 2008.

[10] R. Poovendran and D. Von Oheimb, "Network-Enabled Commercial Airplane Operations," pp. 1–7.

[11] "FAA: Slammer didn't hurt us, but other attacks coming | Network World." https://www.networkworld.com/article/2339600/faa--slammer-didn-t-hurt-us--but-other-attacks-coming.html (accessed Apr. 16, 2022).

[12] "US air traffic faces 'serious harm' from cyber attackers • The Register." https://www.theregister.com/2009/05/07/air_traffic_cyber_attack/ (accessed Apr. 16, 2022).

[13] "Report: Hackers broke into FAA air traffic control systems - CNET." https://www.cnet.com/news/privacy/report-hackers-broke-into-faa-air-traffic-control-systems/ (accessed Apr. 16, 2022).

[14] "Istanbul Ataturk International AirportSecurity Affairs." https://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html (accessed Apr. 16, 2022).

[15] "Phishing Scam Targeted 75 US Airports." https://www.informationweek.com/cybersecurity/phishing-scam-targeted-75-us-airports (accessed Apr. 16, 2022).

[16] "Attack On LOT Polish Airline Grounds 10 Flights." https://www.forbes.com/sites/thomasbrewster/2015/06/22/lot-airline-hacked/?sh=403709d0124e (accessed Apr. 16, 2022).

[17] "Main Cyber-Security Challenges in Aviation." https://www.aerotime.aero/articles/25150-main-cyber-security-challenges-in-aviation (accessed Apr. 16, 2022).

[18] "Ukraine says to review cyber defenses after airport targeted from Russia | Reuters." https://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0 (accessed Apr. 16, 2022).

[19] "Cathay Pacific Cyber Attack Is World's Biggest Airline Data Breach." https://www.insurancejournal.com/news/international/2018/10/26/505699.htm (accessed Apr. 16, 2022).

[20] "British Airways Says 'Sophisicated' Hacker Stole Data on 380,000 Customers." https://www.insurancejournal.com/news/international/2018/09/10/500566.htm (accessed Apr. 16, 2022).

[21] "Delta, Sears Report Data Breach by Service Provider." https://www.insurancejournal.com/news/national/2018/04/05/485440.htm (accessed Apr. 16, 2022).

[22] "Brit airport pulls flight info system offline after attack by 'online crims' • The Register." https://www.theregister.com/2018/09/17/bristol_airport_cyber_attack/ (accessed Apr. 16, 2022).

[23] "Air Canada suffers major app data breach of 20,000 customers - Digital Journal." https://www.digitaljournal.com/business/air-canada-in-major-app-data-breach/article/530763 (accessed Apr. 16, 2022).

[24] "Boeing hit by WannaCry virus, but says attack caused little damage | The Seattle Times." https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/ (accessed Apr. 16, 2022).

[25] "Airbus Statement on Cyber Incident | Airbus." https://www.airbus.com/en/newsroom/press-releases/2019-01-airbus-statement-on-cyber-incident (accessed Apr. 16, 2022).

[26] "Ransomware attack on Albany Airport on Christmas 2019 - Cybersecurity Insiders." https://www.cybersecurity-insiders.com/ransomware-attack-on-albany-airport-on-christmas-2019/ (accessed Apr. 16, 2022).

[27] "Air NZ faces data breach after staff accounts phished." https://securitybrief.co.nz/story/air-nz-faces-data-breach-after-staff-accounts-phished (accessed Apr. 16, 2022).

[28] "DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla | Threatpost." https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/ (accessed Apr. 16, 2022).

[29] "Ransomware attack hits ST Engineering's USA aerospace unit | News | Flight Global." https://www.flightglobal.com/aerospace/ransomware-attack-hits-st-engineerings-usa-aerospace-unit/138722.article (accessed Apr. 16, 2022).

[30] "Airline software super-bug: Flight loads miscalculated because women using 'Miss' were treated as children • The Register." https://www.theregister.com/2021/04/08/tui_software_mistake/ (accessed Apr. 16, 2022).

[31] "Chris Roberts who 'hacked a commercial flight' also hacked the ISS | Daily Mail Online." https://www.dailymail.co.uk/news/article-3090288/Security-expert-admitted-FBI-took-control-commercial-flight-bragged-hacker-convention-2012-playing-International-Space-Station-getting-yelled-NASA.html (accessed Apr. 16, 2022).

[32] "Air France plane carrying 228 people disappears in storm over the Atlantic." https://www.smh.com.au/world/air-france-plane-carrying-228-people-disappears-in-storm-over-the-atlantic-20090601-bsua.html (accessed Apr. 16, 2022).

[33] Y. G. Sun, L. Wang, and W. X. Chen, "A sensor of aero-engine real-time fault detection system based on ARM9," *Adv. Mater. Res.*, vol. 591–593, pp. 1470–1474, 2012, doi: 10.4028/www.scientific.net/AMR.591-593.1470.

[34] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing," *Univ. Texas Austin (July 18, 2012)*, 2012.

[35] S. A. P. Kumar and B. Xu, "Vulnerability Assessment for Security in Aviation Cyber-Physical Systems," 2017, doi: 10.1109/CSCloud.2017.17.

[36] Conventions, "Aviation Security : The Role of IFALPA and its Member Associations," no. December, pp. 1–2, 2021.

[37] "ICAO Standards | IHS Markit." https://ihsmarkit.com/products/icao-standards.html (accessed Apr. 16, 2022).