Automatic Aviation: In-Craft Network, Wireless Data Link, And Off-board Systems

Introduction

Aircraft have dynamically become dependent on software that rely on advanced computing, storage, and networking capabilities. The previous chapters had provided an overall assessment of the security risks posed by the ACPS application domain. We had assessed the high-level design of the system and modeled an aviation CPS. In this chapter, you will find a brief security assessment of a CPS aviation domain. As well as, three different subdomains of the CPS aviation domain and to conduct a security analysis. This chapter’s goal is to find potential security concerns in the domain.

Analysis of Selection

Security is a critical component of the aviation industry on top of safety issues [5]. There are many subdomains but this paper's main focus goes to three subdomains which are chosen for analysis: Subdomain one, in-aircraft network which consists of cabin services systems, crew devices, and maintenance systems. Subdomain two, wireless data link which embraces the aircraft device's connectivity. And the last subdomain is off-board systems, which covers air traffic control systems, satellite communications, and airline info services domains.

The security analysis will cover many aspects of the cyber-physical systems of aviation. The analysis segment will involve analyzing sensors, networks, and both cyber and physical processes. Aviation cyber-physical systems need high integration which has motivated us to analyze this integration. This paper comprises a vulnerability assessment that has been conducted for security in aviation cyber-physical systems in (2017).

Security Analysis Results

What is Security Analysis?

Commencing the Security analysis we define it to clarify this segment [6]. Security analysis refers to the process of evaluating the value of securities such as shares and other securities to determine the overall value of the company that will be useful to investors in making decisions.

In-Aircraft Network

Responsibility

First of all, the in-aircraft network subdomain is where the network and services in the aircraft itself are the main concern. Figure 1. shows the architectural view of this subdomain at the upper level of the figure. Security analysis here compromises the security analysis of aircraft control, airline information services, and passenger information and entertainment services. Avionics systems software is exponentially increasing in aircraft models. These systems are

distributed onboard system architecture Refreshing cyber in avionics in such small timeframes is challenging, mainly because of safety concerns, regulatory requirements, and potential airline loss during aircraft update. However, an exponentially increasing software size on aircraft irrefutably requires frequent periodic updates to avionics subsystems[11].

Figure 1. Aviation Subdomains. Ampigethaya, K. and Poovendran, R., (2012). Cyber-Physical Integration In Future Aviation Information Systems. Available at: https://ieeexplore.ieee.org/document/6382416

Affected Assets

- Due to the huge industry, we are covering, the listed assets are the main assets found in the in-aircraft domain:
- Flight operational and planning data, (e.g., aircraft trajectory).
- Passenger personal data, (e.g., passport and personal preferences data).
- Security relevant data, (e.g., digital certificates, keys, credentials, and passwords that protect aircraft information).
- Aircraft information systems include all networked platforms, embedded and crew-carried devices within the aircraft.
- Passengers and crew members.

Security Risks

Security in in-aircraft networks is important because unsecured related assets of this subdomain can lead to catastrophic events. Lack of testing security changes is considered to be a huge mistake because mistesting after the security system or system's policies changes is going to introduce even more risks to the system. In addition to that, here are some risks that may occur in this subdomain:

Data interception

- Denial of service
- Rogue access points
- Ad Hoc
- Data misconfiguration
- SQL injection

To overcome and minimize the security risks, it is better to have a security risk plan, set and use high-security technologies and policies, and train staff to keep updating and checking the security of these critical systems.

Potential Vulnerabilities

As mentioned previously in chapter 2 "Design Analysis" of this project, vulnerabilities in aviation systems can be categorized into four categories: platform configuration vulnerability, platform hardware vulnerability, platform software vulnerability, and platform malware vulnerabilities. In this subdomain, some vulnerabilities of the previous categories found in chapter 2 "Design Analysis" will be referenced here as follows:

- Operating systems and application software patches develop is delayed or not maintained.
- Using the default configurations in the systems or configuration not saved or backed up.
- No protection for the data in Portable Devices.

Wireless Datalink

Responsibility

Secondly, the wireless data link subdomain which mainly uses ADS-B. ADS-B is defined as a surveillance technology in which an aircraft determines its position via satellite navigation and periodically broadcasts it, enabling it to be tracked [10]. Data transfer happens over a certain link protocol that allows data to be transferred from the source to the destination. The control networks must however, exhibit determinism for time-critical operations, (e.g., in terms of end-to-end delay and packet delivery rate) [11]. It is a challenge for wireless networks to benefit off of networked embedded systems while minimizing the risk of damage and disruption of cyber systems.

Affected Assets

- Airspace data, (e.g., ADS-B-In, terrain maps, weather radar, and traffic information on air-ground and air-air communications).
- Security relevant data, (e.g., digital certificates, keys, credentials, and passwords that protect aircraft information).
- Assets also include software, protocols, algorithms, and memory used in hardware and infrastructures in system handling data

Security Risks

In this subdomain, data link is the most vulnerable domain since the connectivity is established wirelessly. The main or most common risk or in other word threats are:

- Data interception.
- Denial of service.
- Rogue access points.

Moreover, figure 2. illustrates more on data link threats and risks.

Figure 2. Data Link Security Risks. Adapted from: Gurtov, A., T, al. (2020). Controller Pilot Data Link Communication Security. Available at: https://www.researchgate.net/publication/325266463_Controller-Pilot_Data_Link_Communication_Security

Potential Vulnerabilities

- Remote access to information and computer science components.
- Dual network interface card connected to the network
- Using plain text while communicating which means unencrypted data.
- Uninstalled intrusion detection and prevention software.
- Data “openly” delivered on a shared communication link.

Off-board Systems

Responsibility

Finally, the third and final subdomain off-board Systems potentially impacts aircraft safety will heavily use commercial-grade hardware and software, which cannot be assured using the existing aviation safety assurances which implicates a gap between safety standards and

cyber advances. Since the aircraft control domain is the most critical in terms of timeliness, correctness, predictability, and safety properties, we focus on this logical domain of the aircraft. Specifically, we focus on the avionics in the aircraft control domain that enable participation in the next-generation ATM systems[11].

The previously mentioned Figure 1. is an illustration of an aircraft system anticipated in the next two decades; it shows network and computing aspects of cyber onboard and off-board aircraft. In addition, it shows the related stakeholders of these domains.

Affected Assets

- Aircraft digital content, (e.g., software, airline logistics).
- Voice communication systems allow transition from analog to digital voice and intelligent voice switching systems over the Internet for air traffic control.
- Radar, ground, and satellite systems.

Security Risks

Since there is a high level of systems integration between aircraft and off-board systems and several aircraft data links connect to off-board systems, the security risk will increase. The following are some examples of security threats or risks in off board system:

- Unauthorized access
- False data injection
- Eavesdropping
- Jamming
- False alarm
- Message deletion, modification
- Disrupt the flow of aircraft

Potential Vulnerabilities

- No physical protection for offboard devices (e.g radar, satellite)
- Unauthorized personnel can physically access the device.
- Weakness in detecting and preventing unauthorized access [7].

Aviation Security Checklist

A checklist is an assist that can be used to reduce failure caused by the shortcomings of human memory and attention. Checklists help guarantee continuity and completeness in the implementation of a project. A typical security analytics practice is to create a project-specific

checklist, or a list of items that most domains have issues in. This list is affected by previous vulnerabilities, what assets are involved and the system's functionality.

For aviation, the checklist is used for ordering specific, essential activities and aircraft configuration changes corresponding to particular environmental conditions during various segments of flight. The aviation checklist will include the assessments of assets based on certain factors:

Domain Security Concerns

A list of objects that a subject can navigate [9].

Domain security concerns

- 1.1 Is risk assessment on passenger behavior done by check-in or agent's staff?
- 1.2 Was the passenger's baggage observed physically when checked in?
- 1.3 Were the physical barriers and security devices for protecting the airport/airside perimeter boundaries checked and experimented on?
- 1.4 Are cryptographic safeguards used for preserving passenger credentials?
- 1.5 Does the system infrastructure deploy prioritization of system critical components?
- 1.6 Are the pre-flight security checks or searches done?
- 1.7 Are specified IDs applied to those who have privileged access?

Exclusive Subdomain Vulnerabilities

A weakness found in the aviation subdomains [9].

Exclusive subdomain vulnerabilities

- 2.1 Is the engineer responsible for installing system devices well trained and aware of the security measure that should be considered?
- 2.2 Is Instrument Landing System signal antanas receiving clear untampered signals?
- 2.3 Is the experimental setup of devices, systems, and lighting completed?
- 2.4 Does the cockpit implement the right access controls to the core components of the system?
- 2.5 Are the Terrain maps reviewed and checked for location precision?
- 2.6 Are the Standard Instrument Departure Routes and Standard Arrival Routes assed for any possible operational issues?
- 2.7 Is the fuel supply arrangements reviewed for any possible fuel quality issues?

Past Vulnerability Mistakes

An error/s that has occured before [5].

Past vulnerability mistakes

- 3.1 Are passenger and crew members checked for Improvised Explosive Devices (IEDs)?

- 3.2 Is the network checked by network security personal to prevent network problems?
- 3.3 Are passenger and passenger carry on luggage examined for chemicals to prevent chemical attacks?
- 3.4 Are devices reviewed, and checked for radiofrequency interferences?

Design Concerns

The worry about the functionality, and the looks of the system [5].

Design concerns

- 4.1 Is the aircraft examined for structural failures?
- 4.2 Has the aircraft functionalities (e.g.: entertainment, AC, exit pathway lights) been tested?
- 4.3 Has the wings, and tails been examined for appropriate performance?
- 4.4 Has the thrust vectoring control been examined beforehand?
- 4.5 Are the temperature sensors inspected for correct measurements?
- 4.6 Are all in-craft engines being examined?

Availability Concerns

The process of data accessibility or is data operating appropriately.

Availability concerns

- 5.1 Has the wireless network activity been encrypted for security reasons?
- 5.2 Are Terrain maps backup available?
- 5.3 Has the emergency plan activity been rehearsed with both passengers and crew members?
- 5.4 Is there a risk management plan?
- 5.5 Have the fire control gadgets been inspected?
- 5.6 Has the catering been checked and sweeped for unlawful components (e.g.: chemicals, weapons)?

Summary

In the paper you will find CPS aviation subdomains. Aviation subdomains are various but the focus was on three subdomains only which are: in-craft network, wireless data link, and off-board system. The purpose of choosing subdomains is to apply security analysis on them, and to illustrate their vulnerabilities, countermeasures, and attacks that may occur on them. Moving on to the aviation-specific checklists which was created depending on five factors which are: domain security concerns, executive subdomain vulnerabilities, past vulnerability mistakes, design concerns, and availability concerns. The security analysis segment concerns were all about how all subdomains shared the same level of security, and vulnerabilities.

Conclusion

All in all, aviation CPS domain consists of various subdomains, this paper had chosen to

mention three particular ACPS subdomains which are: in-craft network, wireless data link, and off-board systems. The purpose of this last chapter is to analyze the security of the chosen subdomains and to create aviation-specific checklists. Ultimately this is the last chapter of this ACPS project.

References

1. K. Sampigethaya and R. Poovendran, 'Aviation Cyber-Physical Systems: Foundations for Future Aircraft and Air Transport,' in Proceedings of the IEEE, vol. 101, no. 8, pp. 1834-1855, Aug. 2013. https://ieeexplore.ieee.org/abstract/document/6480779
2. Boeing Engineering, Operations, and Technology “Cyber-Physical Systems – An Aerospace Industry Perspective”. https://labs.ece.uw.edu/nsl/aar-cps/winterrev4.pdf
3. Andrew J. Kornecki, Embry-Riddle Aeronautical University Janusz Zalewski, Florida Gulf Coast University. Software Security in Aviation https://pdfs.semanticscholar.org/67b7/d3d559a291b6b7bb8c64a8f629c8ba317194.pdf
4. Lintelman, S., Sampigethaya, K., Li, M., Poovendran, R. and Robinson, R., n.d. High Assurance Aerospace CPS & Implications For The Automotive Industry. [ebook] Seattle: Network Security Lab (NSL), University of Washington. Available at: https://labs.ece.uw.edu/nsl/papers/HCSS-08.pdf
5. Kumar, S. and Xu, B., 2017. Vulnerability Assessment For Security In Aviation Cyber-Physical Systems. [ebook] USA: IEEE 4th International Conference on Cyber Security and Cloud Computing. Available at: https://www.researchgate.net/publication/318669860_Vulnerability_Assessment_for_Security_in_Aviation_Cyber-Physical_Systems
6. N.d., 2020. Security Analysis. Available at: https://www.wallstreetmojo.com/security-analysis/
7. Aviation News - Aviation Voice. 2020. Cabin Services System Archives - Aviation News - Aviation Voice. [online] Available at: .
8. Harison, Elad & Zaidenberg, Nezer. (2018). Survey of Cyber Threats in Air Traffic Control and Aircraft Communications Systems. 10.1007/978-3-319-75307-2_12.
9. Aviation News - Aviation Voice. 2020. Cabin Services System Archives - Aviation News - Aviation Voice. [online] Available at: .
10. N.d, n.d. Airport Security Audit Report Checklist. Available at: http://www.cassoa.org/cassoa/wp-content/uploads/2017/10/Att001-R-Airport-Audit-checklist.pdf
11. Securitymagazine.com. 2020. [online] Available at:
12. Sampigethaya, K. and Poovendran, R., 2012. Cyber-Physical Integration In Future Aviation Information Systems. [ebook] Available at:
13. Gurtov, A., Polishchuk, T. and Wernberg, M., 2020. Controller–Pilot Data Link Communication Security. [ebook] Available at: