Bachelor thesis
Computer Science

Radboud University

Secure Location Verification for ADS-B

Author:
Stijn Meijer
s4277163
info@stijnmeijer.nl

First supervisor/assessor:
dr. Veelasha Moonsamy
V.Moonsamy@cs.ru.nl

Second assessor:
dr. Lejla Batina
lejla@cs.ru.nl

June 24, 2016

ABSTRACT

Automatic Dependent Surveillance-Broadcast (ADS-B) will likely replace radar as the backbone of Air Traffic Management (ATM) systems. Research has shown that the current ADS-B implementation is prone to critical security vulnerabilities on its data link. Various countermeasures already exist, either aiming at adding authentication to the data link or at verifying location claims [1]. This thesis focuses on the latter category, namely Secure Location Verification, and examines for six existing solutions whether they are safe and complete. The security assessment is carried out based on the OWASP Top 10 Web Application Security Risks of 2013 [2], in order to structurally search for weaknesses that remained undiscovered in previous research. For each technique, we give cautions and recommendations. We also generally recommend to employ data fusion with radar or multilateration data, and further applying Kalman filtering, traffic modeling and/or an emasculated variant of group verification.

PREFACE

In front of you is the thesis "Secure Location Verification for ADS-B". This is the result of the study of the security aspects of Automatic Dependent Surveillance-Broadcast (ADS-B) for half a year, which was a requirement to obtain the Bachelor's degree.

The aviation industry is well known for its impressive safety record. When I found out that computer security experts expressed major concerns around the security of ADS-B, it immediately caught my attention. I want to thank Nicky for pointing this out to me. From the beginning of the research, I wanted to contribute to further improve aviation safety.

During the Research Methods course, I was able to perform some background research on the topic of securing the ADS-B data link. I want to thank my fellow students – Willem and Ivar in particular – and the teachers for their feedback and suggestions.

After I finished the Research Methods course, I could formally start this research project. Especially the research of Strohmeier et al. [1] has been of great value to me. I want to thank Veelasha and Lejla for the feedback and guidance I received. Especially picking the right method and adhering to the right structure would have been very difficult on my own.

During the project, I got the opportunity to get in contact with aviation and defence experts. I want to thank Erik and Gosse for getting us in touch. Moreover, I want to thank René, Nico, Theo, Judith, Piet, and Bart for their sincere attention, feedback and suggestions. You have had an important influence on my conclusions.

Finally, I also want to thank my girlfriend, family, friends, fellow students and the course coordinator for their (intensive) support, questions, and suggestions. Without you, I might not have been able to complete this project, my bachelor's, and the Honours programme.

I hope the right choices are made to preserve the safety record of the airline industry.

I wish you much reading pleasure.

Stijn Meijer

Nijmegen, June 24, 2016

CONTENTS

1

INTRODUCTION

Traditional civil aviation systems are being replaced by more modern systems, utilizing today's technological possibilities. Automatic Dependent Surveillance-Broadcast (ADS-B) systems enable aircraft to periodically broadcast information about themselves, such as their satellite-based location, velocity, identification and intent [3]. More specifically, the subsystem broadcasting information to ground stations and other aircraft is called *ADS-B Out*, while the subsystem that processes and shows other aircraft's ADS-B information in the cockpit is called *ADS-B In*. Both subsystems combined can assist pilots by creating a common situational awareness, which enables pilots to make decisions with full awareness of impact on other users [4]. Other advantages of ADS-B over traditional radar systems are reduced maintenance costs and a larger covered area. Moreover, the data is public and can be viewed by everyone.

ADS-B systems have already been deployed in a large amount of countries and it is likely that ADS-B will ultimately replace radar as backbone of Air Traffic Management (ATM) systems in various regions. Moreover, the American Federal Aviation Administration (FAA) mandates aircraft in the US to be ADS-B ready by 2020 [4].

Attacks on ADS-B can, in a very worse case, let pilots react in a way that unnecessarily endangers the aircraft and many people's lives. Critical aerospace systems, such as the traffic collision avoidance system (TCAS), rely on ADS-B data. Moreover, advanced attacks could force airports or airspaces to (partially) shut down. Between 1981 and 1994, the FAA developed a new air traffic control (ATC) system. The implementation failed and caused many delayed flights. For the American airliners alone, the resulting loss was $50 billion (passenger detriment excluded) [5]. Attacks on ADS-B can result in both loss of life, economic loss, as well as other implications such as reduced human mobility.

The integral security of ADS-B comprises of at least three main aspects. Firstly, all ADS-B equipment must be implemented securely and correctly. Secondly, the ADS-B data link between airplanes and ground stations, and airplanes mutually, must be secure. Thirdly, as airborne participants mainly rely on the Global Navigation Satellite System (GNSS) to retrieve their (GPS-)location, the communication between airplanes and satellites must be secure. In this thesis, we will solely focus on the second one: the security of the ADS-B data link between airplanes and ground stations, and airplanes mutually.

The current version of ADS-B's data link has serious security concerns. Most importantly, it does neither incorporate authentication between airplanes and ground stations, nor does it incorporate authentication between airplanes. As a result, fraudulent ADS-B data can be easily injected. Moreover, the data link can easily be jammed and even particular messages can be deleted. Combining these attack vectors, seemingly legitimate messages can be manipulated in a sinister way.

In 2014, Strohmeier et al. [1] reviewed the available research on the topic of securing the ADS-B data link, in particular, and air traffic control communication. According to their survey, all-encompassing security requires new message types and/or completely new protocols to be defined, considering authentication right from the beginning. At the same time, they consider the fact that the invention, certification and large-scale deployment of air-traffic systems takes decades. This implies that it would take decades to provide complete security to this vital air-traffic infrastructure. Therefore, since the ADS-B data link would remain critically insecure for decades, waiting for a new protocol that incorporates authentication is not an option.

Suspicious ADS-B participants could be asked to switch to the connection-oriented and more secure ADS-C (ADS-Contract). However, connection-oriented protocols like ADS-C lack most of the advantages of the paradigm change with ADS-B, specifically on cost, scalability and ease of use [1]. In military communications, the cryptographically secure Mode 4 and Mode 5 are used. The latter adopts the ADS-B broadcast capability, so participants can announce their presence without a prior query [1]. However, cost, scalability and ease-of-use once again stand in the way of widespread usage in commercial aviation [1]. Therefore, both ADS-C and Mode 4 / Mode 5 seem to be no viable alternative for ADS-B in commercial aviation, and will not be discussed further in this research.

Most of the danger that results from the injection or modification of ADS-B messages, lies in incorrect location data. Therefore, verifying location claims made by ADS-B participants would not prevent an attack, but at least reduce the danger of any attack. Strohmeier et al. [1] divide the approaches in ADS-B security in two main classes: Secure Broadcast Authentication and Secure Location Verification. The latter class aims at verifying (or at least estimating) whether location claims made by ADS-B participants are genuine, and will be the focus of this thesis.

A major part of the ADS-B business case is attributed to the savings generated by decommissioning or reducing reliance on conventional radar systems [6]. Hence, as a short-term solution, Secure Location Verification could cope with various attacks and could be implemented if it is cost-effective enough to preserve the initial financial incentive ADS-B had to fulfill.

The 2014 survey by Strohmeier et al. [1] covered six countermeasures under the umbrella of Secure Location Verification. Known attacks, namely (I) multilateration, (II) distance bounding, (III) Kalman filtering, (IV) group verification, (V) data fusion and (VI) traffic modeling were summarized, and their advantages and disadvantages described. In this thesis, we will assess the security of the aforementioned six techniques in a more structured manner. To this end, a top 10 of the most prominent web application security risks provided by OWASP is chosen. For each Secure Location Verification technique, we will present a weakness (by example) for each item of the OWASP Top 10 web application security risks of 2013 [2]. Clearly, Secure Location Verification in general is not a web application, but the OWASP list remains the best vulnerability list that can be applied to such a broad security topic. It contributes to the structured fashion of identifying security weaknesses, which may expose vulnerabilities that were not thought of by other authors.

The remainder of this thesis is structured as follows. We start with a review of existing work, presented in chapter 2, on the topic of ADS-B data link security, and, more specifically, Secure Location Verification. The survey by Strohmeier et al. [1] will be at the basis of this chapter. In chapter 3, the security assessment by applying the OWASP Top 10 is described. The resulting recommendations are given both per technique and in general in chapter 4. We conclude the thesis in chapter 5.

2

LITERATURE REVIEW

In this chapter we will review existing work on the security of the Automatic Dependent Surveillance-Broadcast (ADS-B) data link. In the first section we will review an attacker model in the context of the ADS-B data link, while section 2.2 will describe existing countermeasures – and more specific the six Secure Location Verification techniques.

2.1 ATTACKER MODEL

Various attacks on the Automatic Dependent Surveillance-Broadcast (ADS-B) data link have been suggested, and many have already been proved to exist in practice. In 2014, Strohmeier et al. [1] provided the following attacker model in the context of ADS-B data link vulnerabilities:

Eavesdropping: As ADS-B is using unsecured messages over an inherently broadcast medium, it is possible to eavesdrop on the ADS-B data link. The privacy implications of this passive attack aside, eavesdropping can form the basis of more sophisticated active attacks. These problems have been shown in [7]–[9].

Jamming: An adversary communicating with sufficiently high power on the 1090MHz frequency can disable a single ground station or aircraft or an entire area from sending/receiving ADS-B messages. Such attacks have been described in further detail in [7]–[10]. Reactive jamming, targeting only packets which are already in the air, has also been proven feasible by [11]. Concrete attacks [9] are `Ground Station Flood Denial` and `Aircraft Flood Denial`.

Message injection: Since no authentication measures are in place at the data link layer, it is possible to inject non-legitimate messages into the air-traffic communication system. This was shown in [7]–[9]. Kunkel et al. [12] also demonstrated that it is feasible to conduct such an attack with limited knowledge, using cheap and simple technological means. The lack of authentication also induces a lack of non-repudiation, since every node can deny having broadcasted any (false) data and/or claim having received conflicting data, making any kind of liability impossible. Concrete attack instances that use message injection include [9] `Ground Station Target Ghost Injection /Flooding` and `Aircraft Target Ghost Injection/Flooding`.

Message deletion: Interference can be used to physically "delete" messages from the ADS-B data link. The interference can be either destructive (sending the inverse of the legitimate sender's signal and thus cancelling it out) or constructive (causing sufficient bit errors in the message for it to be dropped). Only in the latter case the receiver might still notice that a message has been sent, depending on the implementation and the circumstances. This has been shown by [7] and [9]. Message deletion is key to the `Aircraft Disappearance` attack.

Message modification: An adversary can utilize two methods to modify messages during transmissions over the physical layer. The attacker can send a high-powered signal to replace part or all of the target message (overshadowing), or apply bit-flipping. Alternatively, the attacker can use a combination of message deletion and message injection. The feasibility of message manipulation has been shown in [7], [8], [13] and [14]. Concrete attack examples are [8] `Virtual Aircraft Hijacking` and `Virtual Trajectory Modification`.

2.2 EXISTING COUNTERMEASURES

In the last decade various countermeasures for the attacks we described in section 2.1 have been proposed. Some of the proposed techniques aim at securing the ADS-B data link, while others focus on verifying location claims made by ADS-B participants. Strohmeier et al. [1] call the first paradigm *Secure Broadcast Authentication* (section 2.2.1), and the second one, *Secure Location Verification* (section 2.2.2). The concept of their taxonomy is shown at Figure 1, indicating the distinction between the two classes and the proposed techniques within each class.

In the remainder of this section, we will focus on the Secure Location Verification techniques. However, for completeness we will also briefly mention the key concepts of the proposed Secure Broadcast Authentication techniques.

2.2.1 *Secure Broadcast Authentication*

Countermeasures within the Secure Broadcast Authentication paradigm aim at introducing an authenticated data link for ADS-B. Some of these techniques use cryptographic schemes, while others utilize non-cryptographic techniques, such as fingerprinting. Whilst some researchers designed schemes for ADS-B specifically, others seek to apply methods that are in place for other unidirectional broadcast schemes, typically for wireless sensor networks or VANETs [1].

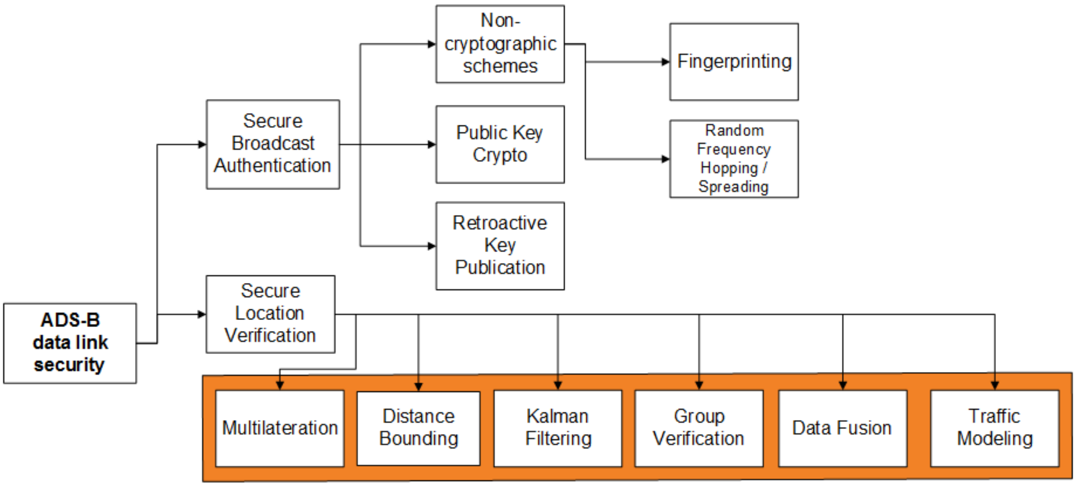

Figure 1: Taxonomy of ADS-B Security based on [1]. The security of the techniques within the coloured box will be assessed in section 3.2.

Secure Broadcasting Authentication techniques can be further divided in three main classes: non-cryptographic schemes, public key crypto, and retroactive key publication. We will now briefly explain the key concepts of each class.

Non-cryptographic schemes

Strohmeier et al. [1] describe two main non-cryptographic schemes for the physical layer:

Fingerprinting comprises of various methods for wireless user authentication and device identification. These methods are based on either hardware or software imperfections, or characteristics of the wireless channel that are hard to replicate. The goal is to distinguish suspicious traffic from legitimate traffic, and machine learning techniques can be utilized to this end. This however does not provide surefire security. Hence, fingerprinting can only be used as an estimate of which traffic is legitimate and which is not.

Randomized / Uncoordinated Frequency Hopping / Spreading are techniques to improve protection against malicious narrow band and pulse jamming as well as eavesdropping. They require pre-shared secret codes, which will presumably not stay secret for long when utilized on a world-wide scale. Hence, these techniques are not a viable option for world-wide deployment.

Public key crypto

ADS-B is not a 'well-connected' network, hence key distribution and management is hard. Keys cannot be exchanged in real-time, restricting the use of symmetric cryptography [15]–[17]. Thus, we look to public key crypto as it distinguishes between private and public keys, of which a public key could be published beforehand.

The smallest and thus best Public Key Infrastructure (PKI) solution is the elliptic curve variant of Digital Signature Algorithm (DSA), ECDSA. However, ECDSA, and PKI schemes in general, require a complex construction of a certificate authority (CA), producing a significant amount of additional traffic over the ADS-B data link for the verification of certificates. This decrease in operational capacity on the 1090 MHz frequency is potentially crippling [4] [17], preventing the widespread usage of ECDSA.

Ziliang et al. proposed a concrete PKI solution for data authentication in ADS-B/UAT based on Elliptic Curve Cipher and X.509 certificates [18].

Samuelson and Valovage [19] propose an implementation of a PKI scheme in which a hash is used to create a message authentication code (MAC). They claim it can be extended to full encryption, but no further details are publicly available.

Retroactive key publication

As a variation on traditional asymmetric cryptography, Strohmeier et a. [1] look at Retroactive Key Publication, the technique of having senders retroactively publish their keys which are then used by receivers to authenticate the broadcast messages. Any broadcasting entity produces an encrypted MAC which is then sent along with every message. After a set amount of time or messages, the key to decrypt this MAC is published. All listening receivers, who have buffered the previous messages, can now decrypt the messages and ensure the continuity of the sender over time.

An implementation of such an efficient broadcast authentication protocol that is able to cope with packet loss and real-time applications, is the TESLA (Timed Efficient Stream Loss-Tolerant Authentication) protocol [20]. The μTESLA broadcast authentication protocol is the adaptation of TESLA for wireless sensor networks, providing authenticated broadcast for these severely resource-constrained environments [21]. Since the available resources on the ADS-B data link are limited, μTESLA would be of interest to ADS-B.

2.2.2 *Secure Location Verification*

Securing ADS-B communication would imply securing the location data – provided that planes are able to retrieve their correct GPS locations. Another approach to ADS-B security is to double-check the authenticity of location claims made by all ADS-B participants. In the following subsections we will cover the different techniques within Secure Location Verification, as described by Strohmeier et al. [1].

Multilateration

Multilateration utilizes antennas on four or more known locations cooperating with each other to determine the origin of an ADS-B signal, using a purely geometric task by comparing the time the signal arrived at the different antennas. Various US airports already use multilateration in the field, for instance the ASDE-X system [22], which is also being rolled out to Europe with the CASCADE project. Multilateration, also known as MLAT, cannot only be applied in airport-scale situations, but also in entire airspaces. In the latter case it is being referred to as Wide Area Multilateration (WAMLAT or just WAM). As the area being monitored increases, a centralized multilateration infrastructure can become useful [23].

Provided that the antennas have been placed on strategic locations [24], multilateration can estimate both latitude and longitude well. However, especially in the case of wide area multilateration, aircraft altitude estimates can be unsatisfying. Additionally, angle-of-arrival measurements can be used to improve height estimations [25].

A major advantage of multilateration is that it uses existing communication, thus no additional messages are required. Unfortunately, the accuracy of multilateration in practice deteriorates over long distance. Covering vast open spaces and oceans was one of the reasons driving the development and deployment of ADS-B. Hence it can be considered a problem that multilateration cannot easily be applied in those regions.

Smith et al. [6] are one of the groups having conducted a practical study on multilateration of ADS-B signals. They examined multilateration as a method to backup and validate ADS-B communication. Other proof of concepts and test beds were built by [26], by [27] in a war-zone in Afghanistan, by [28] in the North Sea, and by [29] in the Gulf of Mexico.

Distance Bounding

Distance bounding [30] is a cryptographic protocol that verifies whether some prover is within a certain physical distance of some verifier. This is done based on the universally valid fact that electromagnetic waves travel roughly at the speed of light. Hence, distance can be computed based on the elapsed time between the verifier's challenge and the corresponding response by the prover. The calculation's result then serves as an upper-bound for the actual distance. When performed by various trusted entities, the verifiers can collaborate and apply trilateration to determine the prover's location.

Various practical attacks on distance bounding exist, such as the distance fraud, mafia fraud and terrorist fraud relay attacks [31], as well as the distance hijacking attack [32]. Some countermeasures already exist as well, for instance the secure distance bounding mechanism for VANETs by Song et al. [33]. A secure multilateration scheme based on distance bounding is developed by Chiang et al. [34], [35]. Theoretically it can detect false location claims with a high rate of success, but the practical problems that stem from combining these two protocols seem hard to overcome. Another problem of the distance bounding protocol is the time the localization takes, combined with the environment of moving targets. Tippenhauer and Čapkun [36] showed that it takes about 600ms to perform a full localization. When a target is moving at a speed of only 500 km/h, this means that he already moves 75 m during the localization process. Another main disadvantage of distance bounding is that it requires a response by the prover on the verifier's challenge. Thus, existing ADS-B equipment must be altered to support this new protocol paradigm.

Kalman Filtering

Kalman filtering [37] tries to statistically and optimally predict future states of the measured variables of the underlying system. It can for instance be used for smoothing location data. The technique plays a crucial role in the multilateration approach, sorting out noisy signals and smoothing over missing data. It is also used to filter and verify the state vectors and trajectory changes reported by ADS-B aircraft and conduct plausibility checks on these data [38]. Krozel et al. [39] demonstrate that Kalman filtering can be applied to test whether an aircraft's motions are in line with its ADS-B intent.

Kalman filters can be misled by a frog boiling attack [40] in which the attacker is jamming the legitimate signal while continuously transmitting a (increasingly) slightly modified position. The fact that Kalman filters can be tricked by such an attack (provided it is carried out slowly enough) exposes a general weakness of the technique. Still, it greatly increases the attack's complexity. The required storage and processing of historical data at every receiver also opens up more DoS-possibilities, but most installations in ground stations and airplanes will be sufficiently powerful.

Group Verification

Group verification [41] aims at securing the airborne ADS-B IN communication by employing multilateration done by a group to verify location claims of non-group members in flight. While classical multilateration is done by ground-based antennas, group verification operates by groups of 4 or more mutually authenticated airplanes. Kovell et al. [42] investigated whether the US airspace is suitable for group verification techniques. They found that around 91% of aircraft at a given time could be part of a sufficiently large group of at least 4 aircraft.

A downside of group verification are the many additional messages required to implement the verification and trust process. The group concept would require a new protocol, replacing ADS-B's unidirectional broadcast protocol. Establishing trust to form a new group and avoiding malicious aircraft is very complicated as well. Moreover, the performance of the system in reaction to intelligent intentional jamming of some or all communication would have to be considered. Still, the group concept would significantly increase the difficulty and engineering effort of certain airborne attacks.

Data Fusion

Data fusion is aggregating data from various independent systems. Applied to ADS-B security, the literature proposes to check positional data obtained from within the system against data from other, independent sources. For example, Baud et al. [43] describe the fusion of radar and ADS-B data and show that this improves the quality of tracking in practice. External data that can be combined with the internal ADS-B data can for instance stem from multilateration, traditional primary radar systems or flight plans. Liu et al. [44] describe an algorithm to fuse sensor data (primary and secondary radar as well as multilateration) and flight plan information together for general fault detection. Such verification can provide a way of knowing if some of the involved systems work outside normal parameters, be it from a malicious form or not. Machine learning can be applied to detect anomalies in received information and to assess the data's trustworthiness (as shown in eg. [45]), triggering technical or non-technical procedures in response.

Data fusion relies on a two-out-of-three approach, which is a widely accepted best practice for processes crucial to safety and security. Data fusion is already employed in practice (eg. in the ASDE-X system) and a data fusion apparatus looking to improve ADS-B security has been patented [46]. The main advantage of data fusion is its compliance with legacy systems, including the current ADS-B protocol. The cost for the additional, generally redundant, systems remain a downside.

Traffic Modeling

Traffic modeling uses historical data and machine learning to create a model of a map of each ground station. The technique can determine whether certain air traffic is abnormal, based on eg. heatmaps or by detecting consecutive packets containing certain unchanged variables, indicating a ground-based attacker. Xia et al. [47] propose an algorithm that could be performed by any node that has received enough measurements. Moreover, an intrusion detection system can utilize numerous comparably simple rules as potential red flags. This way, traffic modeling can indicate unrealistic behaviour that should be further investigated either by a human or by other technical means. For example, when the data provided by an ADS-B participant technically of physically cannot be correct. Having to consider a large number of the aforementioned red flags will increase the attacker's risk of causing an alarm, as well as increase the cost and complexity of the attack.

Leinmuller et al. [48] describe various potential red flags. Examples are the `Acceptance Range Threshold`, which will set of an alarm when a signal is received from a sender that claims to be so far away, that the signal should not have successfully arrived in the first place, and the `Mobility Grade Threshold`, which marks aircraft that claim to be flying faster than they technically can.

3

SECURITY OF SECURE LOCATION VERIFICATION

In this chapter, we assess the security of Secure Location Verification based on the OWASP Top 10 most critical web application security risks (2013) [2]. In the first section, we theoretically discuss the Top 10 list and in the second section, we apply the list to Secure Location Verification.

3.1 OWASP TOP 10

The OWASP Top 10 for 2013 [2] is based on datasets from firms that specialize in application security. This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications. OWASP selected and prioritized the Top 10 items according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact estimates. The 2013 list comprises the following threats, ordered in descending risk:

A1 *Injection*: When untrusted data is sent to an interpreter as part of a command or query, injection flaws could occur. The interpreter can be tricked by the attacker's hostile data into executing unintended commands or accessing data without proper authorization.

Since the insertion of illegitimate aircraft data is the largest risk we consider in this paper, and because this type of attack best fits within the injection category, we will also consider the insertion of data (not necessary triggering the execution of certain commands) within this threat.

A2 *Broken Authentication and Session Management*: When authentication functions are not implemented properly, attackers could compromise passwords, keys or session tokens, or could assume other users' identities.

A3 *Cross-Site Scripting (XSS):* When an application takes untrusted data and sends it to a web browser without proper validation or escaping, XSS flaws could occur. The victims' browser could execute scripts that were injected by the attacker, that could hijack user sessions, deface web sites or redirect the user to malicious sites.

A4 *Insecure Direct Object References:* When a developer exposes a reference to an internal implementation object, such as a file, directory or database key, this is called a direct object reference. It is insecure when the object does not have an access control check or other protection, as attackers can manipulate these references to access unauthorized data.

A5 *Security Misconfiguration:* If secure settings are not defined, implemented and maintained, or if software is not kept up to date, a security misconfiguration occurs.

A6 *Sensitive Data Exposure:* When sensitive data is not given extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser, sensitive data exposure occurs.

A7 *Missing Functional Level Access Control:* When applications do not perform the same access control checks on the server side when a function is accessed as they do on the client side (eg. by displaying/hiding UI elements), functional level access control is missing. If requests to functionalities are not verified properly, attackers will be able to forge requests in order to access functionality without proper authorization.

A8 *Cross-Site Request Forgery (CSRF):* When a logged-on victim's browser sends a forged HTTP request to a vulnerable web application (including the victim's session cookie and any other automatically included authentication information), a CSRF attack occurs. The victim's browser is forced to generate request which the vulnerable application assumes to be sincere requests from the victim.

A9 *Using Known Vulnerable Components:* If a vulnerable component (such as libraries, frameworks and other software modules; often running with full privileges) is exploited, such an attack can facilitate serious data loss or server takeover.

A10 *Unvalidated Redirects and Forwards:* When untrusted data is used to determine destination pages, unvalidated redirects and forwards occur. Victims could be redirected to phishing or malware sites and forwards could be abused to access unauthorized pages.

3.2 ASSESSMENT SECURE LOCATION VERIFICATION

In this section we will use the OWASP Top 10 as a checklist to review whether a technology that aims at providing Secure Location Verification for ADS-B is safe against all of the OWASP Top 10's threats. Moreover, we will give an example of a (concrete) vulnerability where relevant. We will do this for each technology within the Secure Location Verification paradigm, namely for multilateration, distance bounding, Kalman filtering, group verification, data fusion and traffic modeling.

3.2.1 *Multilateration*

A1 *Injection*: The multilateration system will detect fraudulent location data, but cannot verify that the identity provided by a certain ADS-B participant is genuine (see 3.2.1's multilateration example, and 3.2.1 threat A2). However, when signals from the multilateration antennas are sent to the central processing unit over a badly encrypted network, unvalidated data can still be injected. A Denial of Service (DoS) attack on the multilateration infrastructure (see 3.2.1 threat A9) is also a risk, disabling the location validation system and thereby re-enabling the injection of counterfeit location data.

A2 *Broken Authentication and Session Management*: ADS-B participants can assume bogus identities. For instance, a drone equipped with an ADS-B transmitter can claim to be a jumbo jet as long as its location claims are valid (see 3.2.1 threat A7).

A3 *Cross-Site Scripting (XSS):* Not applicable. Multilateration does not take input data that needs to be escaped.

A4 *Insecure Direct Object References:* As communication utilizes various receiving stations (antennas) and a central processing station (CPS). When the link between these communicating entities is implemented in an insecure way, eg. a reference to the CPS's database key is exposed, the security of this database could be breached. In that case, a plane could for instance be removed from the multilateration system, thereby preventing the verification process.

A5 *Security Misconfiguration:* Communication between the multilateration antennas and the ground station should be properly encrypted and authenticated; attempts of tampering with the data should also be detected.

A6 *Sensitive Data Exposure:* While multilateration does not process any sensitive data itself, it is a good idea to keep (some of) the antennas' locations confidential. Since security by obscurity is applied, this will increase the complexity of attacks on the multilateration system.

A7 *Missing Functional Level Access Control:* No access control in the current situation, but a distinction could be made for various sizes of ADS-B participants (ie. drones, general aviation, airlines). For larger planes, a global database could be set up to keep track of their latest known location. This would make it easier to detect bogus identity claims and will increase the complexity of Denial of Service attacks on the antennas.

A8 *Cross-Site Request Forgery (CSRF):* Not applicable. Multilateration does not have an authentication or session management system, and no requests can be sent to the system as well.

A9 *Using Known Vulnerable Components:* When signals from the multilateration antennas are sent to the ground station over a wireless network, this network can be attacked via eg. DoS-attacks, disabling multilateration. Even when a wired network is chosen, data cables and antennas might be compromised. Furthermore, the accuracy of multilateration in practice deteriorates over long distance. Thus, multilateration might not be available on vast open spaces and oceans. Moreover, multilateration is susceptible [49] to multi-path: a situation in which a radio signal reaches the receiving antenna via two paths.

A10 *Unvalidated Redirects and Forwards:* Not applicable. The multilateration system does not have any redirects.

Example (Multilateration).

While one is able to verify whether a location claim made by an ADS-B participant is genuine or not, this does not imply that we know *who* this participant is.

Consider a drone equipped with ADS-B Out that is able to fly at high speed approaching a big city. The location claims it broadcasts are genuine, but the identity is not: it claims to be an American Airlines jumbo jet. With the terrible events of 9/11 in mind, authorities may decide to send out fighter jets, to ground airplanes, or even to evacuate buildings. In the meantime, the drone disappears and is never to be seen again. This could result in significant economical loss, decreased confidence in air transport among the general public, and possibly even panic during any grounding or evacuation.

In practice, however, it seems that many cross-checks (manual *data fusion*) generally happen in such a case.

3.2.2 *Distance bounding*

A1 *Injection*: Distance bounding serves as an upper-bound for the actual distance. Combining multiple verifiers would lead to the same effect as multilateration. Injection of commands or queries that are actually executed is not possible.

A2 *Broken Authentication and Session Management*: ADS-B participants can assume bogus identities. For instance, a drone equipped with an ADS-B transmitter can claim to be a jumbo jet as long as its location claims are valid. (also see 3.2.2 threat A7)

A3 *Cross-Site Scripting (XSS):* Not applicable. Distance bounding does not take input data that needs to be escaped.

A4 *Insecure Direct Object References:* Not applicable. Distance bounding does not refer to any implementation object, such as file, directory or database key.

A5 *Security Misconfiguration:* Various attacks on the distance bounding protocol are known, such as a guessing attack and distance hijacking (see 3.2.2 threat A9).

A6 *Sensitive Data Exposure:* Not applicable. Distance bounding does not process any sensitive data. Comparable to multilateration, the prover's location could be kept secret to increase the attack's complexity.

A7 *Missing Functional Level Access Control:* No access control in the current situation, but a distinction could be made for various sizes of ADS-B participants (ie. drones, general aviation, airlines). For larger planes, a global database could be set up to keep track of their latest known position. This would make it easier to detect bogus identity claims.

A8 *Cross-Site Request Forgery (CSRF):* Not applicable. Distance bounding does not have an authentication or session management system, and no requests can be sent to the system as well.

A9 *Using Known Vulnerable Components:* Various distance bounding protocols are vulnerable to a guessing attack where the malicious power pre-emptively transmits guessed values for a number of response bits, as well as relay attacks (distance fraud, mafia fraud and terrorist fraud) due to latency [31]. Distance Hijacking, where a dishonest prover exploits one or more honest parties to provide a verifier with false information about the distance between prover and verifier, is also a threat [32]. However, performing an attack such as distance hijacking in the ADS-B context seems greatly harder (see 3.2.2's distance bounding example).

A10 *Unvalidated Redirects and Forwards:* Not applicable. The distance bounding system does not have any redirects.

Example (Distance bounding).

The classical distance bounding protocol by Brands and Chaum [30] is susceptible to attacks such as mafia fraud, distance fraud and terrorist fraud [31], as well as distance hijacking [32]. Cremers et al. [32] provided the following summary of these attacks:

Mafia Fraud: In this type of attack, both the prover P and verifier V are honest, and the attack is performed by an external attacker $\mathcal{A}$. The attacker attempts to shorten the distance measured between the honest prover and the verifier.

Distance Fraud: A dishonest prover P will try to shorten the distance measured by the verifier V. This type of attack is executed by the dishonest prover P alone, without collusion with other (external) parties. The attack enables shortening the distance measured by the verifier, as the prover is able to reply too early. This can occur when the protocol allows the prover to send his reply before receiving the challenge.

Terrorist Fraud: A dishonest prover P collaborates with an external attacker $\mathcal{A}$ to convince the verifier V that he is closer than he actually is.

Distance Hijacking: A dishonest prover P convinces a verifier V that P has executed a distance measurement phase with V, whereas this phase has in fact been executed by an honest prover P'. This is done without the cooperation of the honest prover P'. Often this type of attack can be carried out by allowing the honest prover to complete the distance bounding protocol as he normally would, and then by replacing all messages that contain signatures or MACs, with messages signed (or MAC'ed) by the attacker.

We will now assess whether these attacks can be a risk for Secure Location Verification. In the case of mafia fraud, an external attacker could only shorten the distance being measured between a legitimate airplane and the verifier. This seems not very interesting in practice. However, the external attacker could also shorten the distance being measured between the verifier and a *fraudulent* ADS-B participant: the terrorist fraud attack. Cremers et al. [32] observed that the physical distance between the attacker and the verifier is typically small in order for the attacker to be able to shorten the distance. Since the Secure Location Verification implementation of distance bounding utilizes various collaborating verifiers, this attack requires various collaborating attackers, which greatly increases the attack's complexity. This will make it very hard to imitate a trustworthy flight path, especially when distance bounding is combined with other techniques, such as Kalman filtering or traffic modeling.

A successful distance hijacking attack in the context of ADS-B is also not very likely, since this attack only enables a dishonest ADS-B participant P to claim the location of a legitimate aircraft P', or at least a component of its location. With only this ability, it is either nearly impossible to maintain a trustworthy flight path, or the attacker can merely claim to be the legitimate aircraft. The latter would bring the attack back to an *identification* breach, very similar to the problem discussed in multilateration's example 3.2.1.

Merely the distance fraud attack seems to be a risk for ADS-B. However, the required timing precision makes the attack very complex, especially in the situation where multiple verifiers collaborate.

3.2.3 *Kalman filtering*

A1 *Injection*: Injection of counterfeit aircraft data remains possible, but location claims can only differ (increasingly) slightly (see frog boiling attack as demonstrated in 3.2.3's Kalman filtering example). Injection of commands or queries that are actually executed is not possible.

A2 *Broken Authentication and Session Management*: Ghost planes and bogus identities can still be created, as long as they start outside the reach of the Kalman filtering system.

A3 *Cross-Site Scripting (XSS):* Not applicable. Kalman filtering does not take input data that needs to be escaped.

A4 *Insecure Direct Object References:* Not applicable. Kalman filtering does refer to any implementation object, such as file, directory or database key.

A5 *Security Misconfiguration:* Storing and using more historical data could increase the accuracy of the predictions, but could also open up more DoS-possibilities (see 3.2.3. threat A9).

A6 *Sensitive Data Exposure:* Not applicable. Kalman filtering does not process any sensitive data.

A7 *Missing Functional Level Access Control:* An 'access control' system could be introduced, only allowing certain aircraft motions within a certain intent[1]. The system should set off alarms when intent and movement do not match.

A8 *Cross-Site Request Forgery (CSRF):* Not applicable. Kalman filtering does not have an authentication or session management system, and no requests can be sent to the system as well.

[1] *Intent*: Information on planned future aircraft behaviour, which can be obtained from the aircraft systems (avionics).

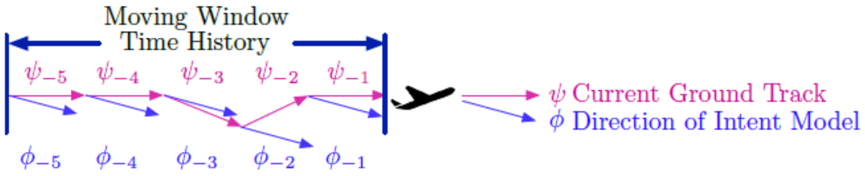
Moving Window
Time History
ψ_{-5} ψ_{-4} ψ_{-3} ψ_{-2} ψ_{-1}
ϕ_{-5} ϕ_{-4} ϕ_{-3} ϕ_{-2} ϕ_{-1}
ψ Current Ground Track
ϕ Direction of Intent Model

Figure 2: Intent verification by Kalman filtering [39].

A9 *Using Known Vulnerable Components:* The required storage and processing of historical data at every receiver opens up more DoS-possibilities, but most installations in ground stations and airplanes will be sufficiently powerful [1].

A10 *Unvalidated Redirects and Forwards:* Not applicable. The kalman filtering system does not have any redirects.

Example (Kalman filtering).

The frog boiling attack, as proposed by Chan-Tin et al. [40], describes the situation where an adversary jams the original signal, and inserts counterfeit data while consistently operating within the threshold of rejection. In Figure 2, a typical example of intent verification by utilizing Kalman filtering can be seen.

When an attacker performs the attack slowly enough, the Kalman system will see the injected data as a valid trajectory change. This could be considered as a message modification attack since air traffic control and other aircraft expect this plane to be on a different location than it is in reality. By doing so, aircraft can be given wrong instructions by air traffic control, and systems like the traffic collision avoidance system (TCAS) might take the wrong input or respond in a way it should not respond.

3.2.4 *Group verification*

A1 *Injection*: The newly introduced communication in the new protocol, eg. arranging mutual authentication within the group, could introduce new injection vulnerabilities. Nevertheless, the complexity of injecting false location data is increased significantly.

A2 *Broken Authentication and Session Management*: The in-group mutually authentication must be done thoroughly, which will be a challenge. Moreover, like is the case with multilateration and distance bounding, a verified location does not imply a verified identity.

A3 *Cross-Site Scripting (XSS):* The implementation should be very careful of the possibility of man-in-the-middle attacks, as well as attacks with multiple adversaries (see 3.2.4 threat A9 and 3.2.4's group verification example).

A4 *Insecure Direct Object References:* Not applicable. Group verification does refer to any implementation object, such as file, directory or database key.

A5 *Security Misconfiguration:* As is the case with multilateration, the communication and mutual authentication within group members should be well encrypted and authenticated. Since group verification is bound to use a wireless channel for this communication, the protocol should be resistant against man-in-the-middle attacks.

A6 *Sensitive Data Exposure:* Not applicable. This technique does not handle any additional sensitive data.

A7 *Missing Functional Level Access Control:* All communication within the group should be properly encrypted and authenticated. Without proper authentication, attackers could access functionality without valid authorization. For instance, a fraudulent aircraft could get itself approved by all surrounding groups.

A8 *Cross-Site Request Forgery (CSRF):* The process of mutual authentication and querying (assumed) group members opens up various man-in-the-middle possibilities. Forged requests could be used to carry out such a MitM attack.

A9 *Using Known Vulnerable Components:* The communication between group members is prone to (reactive) jamming. This would cause a (partial) DoS on the group verification system. The system is also unusable in areas with almost no air travel, since no groups can be formed in these areas.

Above all, while not a weakness of the technique itself, the group concept would require a new protocol, replacing ADS-B's unidirectional broadcast protocol. This makes the implementation of group verification harder than the other techniques (since all ADS-B equipment has to be replaced), and makes group verification unsuitable as a short term solution.

A10 *Unvalidated Redirects and Forwards:* Not applicable. The group verification concept does not have any redirects.

Example (Group verification)**.**

A special case of an attack with multiple adversaries occurs when a single adversary utilizes multiple sending antennas, spread around different locations. It can combine timing and signal strength (and therefore reach) to dynamically claim to be on a location of choice, and those claims will still be approved. This attack can occur in both 'standard' multilateration settings, as well as within group verification.

3.2.5 *Data fusion*

A1 *Injection*: The fusion of sensor data (eg. from ADS-B and radar or multilateration systems) with flight plan data will make a quick detection of injected counterfeit data more likely. The two-out-of-three approach will also increase the complexity of the injection attack itself, but does not exclude the possibility of a successful attack. Above all, the various sensor and flight plan data must be properly validated in order to prevent injection attacks.

A2 *Broken Authentication and Session Management*: When ADS-B data is fused with either radar or multilateration data, location claims can be verified. When fused with flight plan data, it becomes viable to make an educated guess to determine whether the actual identity of the aircraft matches the identity it claims to be. However, all data sources that deliver data to the data fusion algorithm need to be properly authenticated (see 3.2.5 threat A7).

A3 *Cross-Site Scripting (XSS):* All sensor and flight plan data must be properly escaped in order to prevent XSS attacks.

A4 *Insecure Direct Object References:* The storage and retrieval of flight plan records should be secure, among others to prevent sensitive data exposure (see 3.2.5 threat A6).

A5 *Security Misconfiguration:* The presence of a security misconfiguration (risk) will depend on the implementation of the fusion application.

A6 *Sensitive Data Exposure:* In some circumstances, detailed flight information can be sensitive. For instance, when a presidential airplane is expected to fly over an airspace that can be considered dangerous. However, due to the transparent nature of ADS-B, some sensitive information may already be public.

A7 *Missing Functional Level Access Control:* Within this technique, it is key to properly verify the legitimacy of the various data sources. When fraudulent data sources can be added to the system, this will bring down the whole security framework. Moreover, the data sources themselves need to properly verify their own input and access control. This applies to the flight plan data source in particular, as it will likely rely on data provided by third parties, such as airliners. It is of fundamental importance to the data fusion concept that all inserted data is legitimate.

A8 *Cross-Site Request Forgery (CSRF):* The presence of CSRF attacks will depend on the implementation of the fusion application.

A9 *Using Known Vulnerable Components:* Vulnerabilities of the various subsystems could be abused (especially the insertion of fraudulent data, as shown in A7). Since the additional, generally redundant, subsystems generate extra financial costs, they may be switched off in the future, undermining the accuracy and effectiveness of the data fusion application.

A10 *Unvalidated Redirects and Forwards:* Not applicable. The data fusion application is unlikely to have any redirects.

3.2.6 *Traffic modeling*

A1 *Injection*: Utilizing various potential red flags will increase the detection likeliness when illegitimate data is inserted.

A2 *Broken Authentication and Session Management*: Traffic modeling can make some basic distinctions, for instance whether some object actually is a plane or some ground station that claims to be a plane. It can also (statistically) decide whether it is logical to have a plane on a certain location. However, a (slightly altered) replay attack can still be performed by any ADS-B participant, claiming a false location. A false identity can still be claimed as well.

A3 *Cross-Site Scripting (XSS):* Not applicable. Traffic modeling does not take input data that needs to be escaped.

A4 *Insecure Direct Object References:* Not applicable. Traffic modeling does not refer to any implementation object, such as file, directory or database key.

A5 *Security Misconfiguration:* As shown at 3.2.6. threat A9, the storage and processing of historical data could open up DoS attack avenues.

A6 *Sensitive Data Exposure:* Exposure of the generated heatmaps could assist an attacker to circumvent this countermeasure. However, since ADS-B data is public, an attacker might also generate a heatmap herself.

A7 *Missing Functional Level Access Control:* Not applicable. Traffic modeling does not have any functionalities that can be accessed from the outside world.

A8 *Cross-Site Request Forgery (CSRF):* Not applicable. Traffic modeling does not have an authentication or session management system, and no requests can be sent to the system as well.

A9 *Using Known Vulnerable Components:* An attacker deliberately causing lots of false alarms as a basis for another attack might be a problem. Moreover, the storage and processing of historical data could open DoS possibilities, as the machine learning algorithm might run out of its capacity when dozens of (fake) planes suddenly pop up.

A10 *Unvalidated Redirects and Forwards:* Not applicable. The traffic modeling system does not have any redirects.

4

RECOMMENDATIONS

4.1 RECOMMENDATIONS PER TECHNIQUE

4.1.1 *Multilateration*

Multilateration is a ground-to-air approach for verifying location claims by using multiple, interconnected, antennas. The air-to-air variant of multilateration is Group verification, and has been discussed in section 4.1.4.

Multilateration's main advantage is its compliance with the existing ADS-B infrastructure, as it is an additional system that does not interfere with existing equipment. Its main disadvantages are the additional costs for the redundant systems and the fact that it only verifies location claims, but does not check aircraft's identities. However, the latter seems to be of lower impact in practice. Aside from jamming attacks, which are very hard to overcome, man in the middle attacks seem to be the most relevant attacks on multilateration. The fact that the technique is susceptible to multipath should be kept in mind as well.

The main recommendations for the multilateration technique, are:

- The complexity of multilateration attacks could be increased by keeping (some of) the antennas' locations confidential.
- The complexity of man in the middle attacks could be increased even further by not (only) considering the time difference of arrival (TDOA), but also the difference in received signal strength (RSS) or angle-of-arrival (AoA) when determining where a signal came from.

4.1.2 *Distance bounding*

Distance bounding servers as an upper-bound for the actual distance between aircraft and ground station. When multiple distance circles collaborate, the actual location of the prover can be found via trilateration: by comparing the *absolute* difference in measurements.

In a broad perspective, distance bounding can be compared to multilateration. A main disadvantage of distance bounding when compared to multilateration, is that it requires new traffic over the data link, while multilateration merely uses existing communication. This also implies that existing equipment must be altered to be able to reply to the verifier's challenges.

Various attacks exist for the distance bounding concept, but many are not very interesting when considering their use for ADS-B. Only the distance fraud attack seems to be of interest to ADS-B, but the attack's complexity is high, and even further when distance bounding is combined with techniques that monitor the ADS-B participant's flight path, such as Kalman filtering or traffic modeling. Therefore, the main recommendation for distance bounding is:

- Combine the distance bounding technique with the Kalman filtering and/or traffic modelling techniques, in order to greatly increase the complexity of any known attacks.

4.1.3 *Kalman filtering*

Kalman filtering attempts to predict an aircraft's future state by applying statistics, and may mark the behaviour as unexpected. The resulting distinction between legitimate and illegitimate-marked aircraft is very much like the traffic modeling technique. Therefore, the main aspects and recommendations for the Kalman filtering technique are given along with those for the traffic modeling technique, in section 4.1.6.

4.1.4 *Group verification*

Group verification is multilateration done by a group.

Should it be implemented, then extra caution should be given to man-in-the-middle attacks. Whilst not suitable in thinly populated airspaces, it could provide both location verification and mutual authentication.

While multilateration itself is compliant to the existing ADS-B infrastructure, group verification is not. It requires a new protocol for mutual authentication between airplanes and for assessing the trustworthiness of others' ADS-B signals. It is likely that ground stations could be added as well, making this a good solution in the long run. For a short-term solution however, it seems unsuitable due to the replacement of ADS-B's unidirectional protocol with a new protocol. While Kovell et al. [42] found that around 91% of aircraft at a given time in the US airspace could be part of a sufficiently large group of at least 4 aircraft, it is very unlikely that all existing equipment will be immediately upgraded. Therefore, this figure is way too optimistic for the current situation, as it takes time to replace existing equipment.

Moreover, the additional bandwidth that is required for the communication within the groups will not be available on the 1090MHz frequency.

The concept could be emasculated to make it available in a shorter period of time, and reduce the amount of messages sent. When the entire group negotiating aspect is removed, aircraft do not need to form trust groups anymore. Instead, they can extend their existing ADS-B broadcast information with details about nearby planes: both their identification and location. Others can then calculate whether this is in line with what they and other aircraft are seeing. This way, it can be detected when fraudulent data is around. Since there can be multiple attackers around, this can only be taken as an indication – similar to Kalman filtering and traffic modeling.

Therefore, the main recommendations for group verification are:

- Emasculate the concept to make it compatible with ADS-B's unidirectional broadcast protocol.
- Consider man-in-the-middle attacks and multiple adversaries.

4.1.5 *Data fusion*

Data fusion can be considered as the backbone of Secure Location Verification techniques. It glues together the different parts of the puzzle. The main potential vulnerability of the system is its input, not only by means of preventing injections, but also by guaranteeing that the received data from other sources is legitimate.

This comes down to two both important and intuitive recommendations:

- The integrity of all data that is provided by the various data sources, as well as the authenticity of the data sources itself, need to be checked.
- The received data must be validated properly.

4.1.6 *Traffic modeling*

Traffic modeling tries to predict an aircraft's future state by applying machine learning, and may mark the behaviour as unusual.

While counterfeit ADS-B participants can be filtered out quite easily by applying this technique, this is not the case in reverse. Thus, when a signal is not marked as being unusual, this does not imply that it is legitimate. Also, some fraudulent aircraft might still fall within the threshold of not being unusual. This is especially the case with replay attacks, wherein the flight path of an earlier, legitimate, flight is being copied.

The general recommendation for both Kalman filtering and traffic modeling, is:

- The Kalman filtering and traffic modeling techniques should only be applied as first filters. Illegitimate ADS-B participants should be marked on the controller's screens, and not just be removed silently.

4.2 GENERAL RECOMMENDATIONS

Most of the Secure Location Verification techniques cover a specific aspect, while data fusion can be considered the main glue between them. Therefore, data fusion is implicit in any complete Secure Location Verification solution, just as it is implicit in the current (manual) handling of suspicious data by air traffic control.

Multilateration and distance bounding are somewhat comparable in their concept. We recommend to choose multilateration as the technique to be implemented, as there are no known attacks on the location verification aspect of multilateration. When a primary radar system is around, for instance because the military forces keep this system operational, multilateration is not necessarily.

Kalman filtering, traffic modeling and the emasculated variant of group verification can be used as warnings, indicating that someone is injecting fraudulent ADS-B data (or, in the latter case, maybe even jamming communication). These techniques greatly increase the complexity of most attacks.

As an alternative, since the world-wide ADS-B coverage is ever expanding, a global database tracking any plane's last known position could be set up. This would prevent the sudden pop-up of an aircraft. The management of such a database could be done by a world-wide trusted aviation authority, such as the ICAO.

5

CONCLUSIONS

Out of the 6 Secure Location Verification techniques we assessed, multilateration is already being implemented in the real world. Other techniques, such as fusing data from various sources are already being utilized by air traffic control (ATC), however mostly by hand. When unusual ADS-B data is seen, it is manually checked against other sources, such as radar and flight plan data. While the (academic) literature might give the impression that ADS-B will replace radar systems, areas with high traffic and a good infrastructure – such as continental Europe – will very likely remain covered by primary radar in the future.

At first glance, the combination of ADS-B and primary radar installations by comparing the screens by hand might seem safe in practice. In the case of fraudulent ADS-B messages being broadcasted, an air traffic controller could cross-check any suspicious ADS-B participant on the radar screen. Controllers are used to seeing some noise on the traditional radar screens, and will recognise aircraft that are off-path. However, the controllers' workload will increase as more fraudulent aircraft are appearing. Moreover, replaying the path a legitimate airplane flew before might not trigger the controller's caution.

To overcome this, (already existing) radar data should be automatically synchronized with ADS-B and even flight plan data (*data fusion*, as this technique is called). In areas where radar systems are no viable option, multilateration could be connected to the data fusion system instead. Fraudulent ADS-B participants will be marked on, or removed from, the screens of air traffic controllers. Kalman filtering and traffic modeling can be added as a first stage of filtering out illegitimate signals, for instance when a certain plane type makes a corner it possibly cannot make, but these techniques can never be trusted as to determine whether a location claim is genuine or not.

The goal of applying the OWASP Top 10 was to structurally search for threats that previously remained undiscovered. While some of the threats of the Top 10 list not always seemed applicable to the Secure Location Verification techniques, in the end they often were. Consider *Missing Functional Level Access Control* when applied to Multilateration. This seems inapplicable, as there is no access control in place, but after thinking about this we were able to come up with the "localization does not imply identification" scenario.

An interesting question for further research is how the aforementioned warnings ATC gets could be best propagated to other airplanes. Further research could also investigate how the various ADS-B data link vulnerabilities directly influence the aircraft's safety, eg. by examining how fraudulent ADS-B data that is being sent through to the traffic collision avoidance system (TCAS) could possibly cause a crash.

REFLECTION

In this chapter, I will briefly reflect on the research process and its outcome. I will identify both aspects that worked well for me, and aspects that did not. Although all experiences are personal, some lessons may be useful to others as well.

From the start of this research project, the goals have been twofold:

1. To meet the requirements for the Bachelor's degree; and

2. To further improve aviation safety.

It seems like I was able to accomplish the first goal, but did I succeed in the second? In order to answer this question, we have to make a distinction between security on one hand, and safety on the other. Since my expertise is computer security, I tend to focus more on (theoretical) security. From this point of view, ADS-B's data link is usually considered insecure. But does this necessarily imply that it is also *unsafe*? The concept of safety kind of describes the applied version of security. Thus, while the ADS-B data link can be considered insecure from a computer security point of view, it can still be safe in (aviation) practice.

In hindsight, I think the best way to further improve the safety of the industry would be a thorough collaboration between theory-oriented computer security academia, and practice-oriented aviation and defence experts. Both disciplines should try to find a balance; both between safety vs. security, as well as between keeping the user in command vs. automating attack detection and reaction.

On a more personal note, I really liked the research topic and the way I was supervised. To topic immediately felt of great importance to me. From the beginning, I wanted to contribute to further improve aviation safety. But when I started the research, I did have a topic, but without a method. I quickly realised that it was unrealistic to perform an actual (attack) experiment, considering the available time frame, as well as the safety and legal issues. As I personally am more practice-oriented, it seemed slightly against my nature to merely perform a literature review.

A highlight in my research was the ability to talk to actual aviation and defence experts. Personally, I think the conclusions arising from this meeting can be considered my biggest contribution to the field. As expressed before, I hope other researchers will follow this example.

BIBLIOGRAPHY

[1] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol", *Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[2] OWASP, *Owasp top 10 2013*, Website OWASP, 2013. [Online]. Available: `http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf`.

[3] F. A. Administration, *14 cfr 91.227 - automatic dependent surveillance-broadcast (ads-b) out equipment performance requirements - final rule*, Code of Federal Regulations, Jan. 2015. [Online]. Available: `https://www.law.cornell.edu/cfr/text/14/91.227`.

[4] H. Yang, R. Huang, X. Wang, J. Deng, and R. Chen, "Ebaa: an efficient broadcast authentication scheme for ads-b communication based on ibs-mr", *Chinese Journal of Aeronautics*, vol. 27, no. 3, pp. 688–696, 2014.

[5] R. N. Charette, "Why software fails", *Spectrum, IEEE*, vol. 42, no. 9, pp. 42–49, 2005.

[6] A. Smith, R. Cassell, T. Breen, R. Hulstrom, and C. Evers, "Methods to provide system-wide ads-b back-up, validation and security", in *Proceedings of the 25th Digital Avionics Systems Conference*, 2006, pp. 1–7.

[7] A. Costin and A. Francillon, *Ghost in the air (traffic): on insecurity of ads-b protocol and practical attacks on ads-b devices*, Whitepaper on website Black Hat USA, 2012. [Online]. Available: `https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf`.

[8] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication", *Applied Cryptography and Network Security*, pp. 253–271, 2013.

[9] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ads-b implementation in the next generation air transportation system", *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011.

[10] L. Purton, H. Abbass, and S. Alam, "Identification of ads-b system vulnerabilities and threats", in *Australasian Transport Research Forum 2010 Proceedings*, 2010, pp. 1–16.

[11] A. Wilhelm and I. Martinovic, "Short paper: reactive jamming in wireless networks: how realistic is the threat?", in *Proceedings of the 4th ACM conference on Wireless network security*, 2011, pp. 47–52.

[12] R. Kunkel, *Air traffic control insecurity 2.0*, Website DefCon 18, 2010. [Online]. Available: `https://www.defcon.org/images/defcon-18/dc-18-presentations/Kunkel/DEFCON-18-Kunkel-Air-Traffic-Control.pdf`.

[13] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel", in *ESORICS 2011*, Springer Berlin Heidelberg, 2011, pp. 40–59.

[14] M. Wilhelm, J. B. Schmitt, and V. Lenders, "Practical message manipulation attacks in ieee 802.15.4 wireless networks", in *MMB & DFT 2012 Workshop Proceedings*, 2012.

[15] W. J. Pan, Z. L. Feng, and Y. Wang, "Ads-b data authentication based on ecc and x. 509 certificate", *Jounal of Electronic Science and Technology*, vol. 10, no. 1, pp. 51–55, 2012.

[16] C. Finke, J. Butts, R. Mills, and M. Grimaila, "Enhancing the security of aircraft surveillance in the next generation air traffic control system", *International Journal of Critical Infrastructure Protection*, vol. 6, no. 1, pp. 3–11, 2013.

[17] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Can cryptography secure next generation air traffic surveillance?", *IEEE Security and Privacy Magazine*, 2014.

[18] Z. Feng, W. Pan, and Y. Wang, "A data authentication solution of ads-b system based on x. 509 certificate", in *27th International Congress of the Aeronautical Sciences, ICAS*, 2010.

[19] K. Samuelson, E. Valovage, and D. Hall, "Enhanced ads-b research", in *Proceedings of the Aerospace Conference, 2006 IEEE*, 2006, pp. 1–7.

[20] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The tesla broadcast authentication protocol", *RSA CryptoBytes*, vol. 5, 2005.

[21] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks", *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[22] J. J. Herrero, J. Portas, J. C. R. C. Corredera, J. Besada Portas, and F. Rodriguez, "Asde and multilateration mode-s data fusion for location and identification on airport surface", in *Radar Conference, 1999. The Record of the 1999 IEEE*, 1999, pp. 315–320.

[23] T. A. S. GmbH, *Ground stations and multilateration*, Website ICAO, Retrieved May 19, 2016. [Online]. Available: http://www.icao.int/APAC/Meetings/2012_SEA_BOB_ADSB_WG8/SP03_Thales%20ADS-B%20Multilateration.pdf.

[24] F. A. Niles, R. S. Conker, M. B. El-Arini, D. G. O'Laighlin, and D. V. Baraban, *Wide area multilateration for alternate position, navigation, and timing (apnt)*, Website FAA, Retrieved May 19, 2016. [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/documents/APNT/media/WAM_WhitePaperFINAL_MITRE_v2.pdf.

[25] G. Galati, M. Leonardi, P. Magarò, and V. Paciucci, "Wide area surveillance using ssr mode s multilateration: advantages and limitations", in *European Radar Conference (EURAD)*, 2005, pp. 225–229.

[26] R. Kaune, C. Steffes, S. Rau, W. Konle, and J. Pagel, "Wide area multilateration using ads-b transponder signals", in *15th International Conference on Information Fusion (FUSION)*, IEEE, 2012, pp. 727–734.

[27] J. Johnson, H. Neufeldt, and J. Beyer, "Wide area multilateration and ads-b proves resilient in afghanistan", in *Integrated Communications, Navigation and Surveillance Conference (ICNS), 2012*, IEEE, 2012, A6–1.

[28] P. Thomas, "North sea helicopter ads-b/mlat pilot project findings", in *Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), 2011*, IEEE, 2011, pp. 53–58.

[29] A. Daskalakis and P. Martone, "A technical assessment of ads-b and multilateration technology in the gulf of mexico", in *Proceedings of the 2003 IEEE Radar Conference*, IEEE, 2003, pp. 370–378.

[30] S. Brands and D. Chaum, "Distance-bounding protocols", *Advances in Cryptology - EUROCRYPT'93*, pp. 344–359, 1994.

[31] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: distance-bounding attacks in wireless networks", *Security and Privacy in Ad-hoc and Sensor Networks*, pp. 83–97, 2006.

[32] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols", in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 113–127.

[33] J.-H. Song, V. W. Wong, and V. C. Leung, "Secure location verification for vehicular ad-hoc networks", in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008*, 2008, pp. 1–5.

[34] J. T. Chiang, J. J. Haas, and Y.-C. Hu, "Secure and precise location verification using distance bounding and simultaneous multilateration", in *Proceedings of the second ACM conference on Wireless network security - WiSec '09*, 2009, pp. 181–192.

[35] J. T. Chiang, J. J. Haas, J. Choi, and Y. Hu, "Secure location verification using simultaneous multilateration", *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 584–591, 2012.

[36] N. O. Tippenhauer and S. Čapkun, "Id-based secure distance bounding and localization", in *Computer Security - ESORICS 2009*, 2009, pp. 621–636.

[37] R. E. Kalman, "A new approach to linear filtering and prediction problems", *Journal of basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[38] D. Fox, J. Hightower, L. Liao, D. Schulz, and G. Borriello, "Bayesian filtering for location estimation", *IEEE pervasive computing*, no. 3, pp. 24–33, 2003.

[39] J. Krozel, D. Andrisani, M. A. Ayoubi, T. Hoshizaki, and C. Schwalm, "Aircraft ads-b data integrity check", in *AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum*, 2004, pp. 1–11.

[40] E. Chan-Tin, V. Heorhiadi, N. Hopper, and Y. Kim, "The frog-boiling attack: limitations of secure network coordinate systems", *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 3, p. 27, 2011.

[41] K. Sampigethaya and R. Poovendran, "Security and privacy of future aircraft wireless communications with offboard systems", in *Third International Conference on Communication Systems and Networks 2011 - COMSNETS 2011*, 2011, pp. 1–6.

[42] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, "Comparative analysis of ads-b verification techniques", Master's thesis, The University of Colorado, Boulder, 2012.

[43] O. Baud, N. Honore, and O. Taupin, "Radar / ads-b data fusion architecture for experimentation purpose", in *9th International Conference on Information Fusion*, 2006, pp. 1–6.

[44] W. Liu, J. Wei, M. Liang, Y. Cao, and I. Hwang, "Multi-sensor fusion and fault detection using hybrid estimation for air traffic surveillance", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2323–2339, 2013.

[45] Y.-C. Wei, Y.-M. Chen, and H.-L. Shan, "Beacon-based trust management for location privacy enhancement vanets", in *13th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2011.

[46] A. E. Smith, *Method and apparatus for improving ads-b security*, US Patent 7,423,590, Sep. 2008. [Online]. Available: `https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US7423590.pdf`.

[47] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets", in *International Conference on Mobile Computing and Networking: Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 1–8.

[48] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad-hoc networks", *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.

[49] J. C. Siu, "Icao concepts and references regarding ads-b, multilateration and other surveillance techniques", in *ICAO/FAA Workshop on ADS-B and Multilateration Implementation*, 2011.