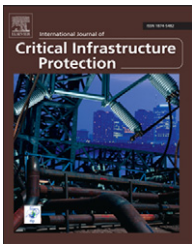
Available online at www.sciencedirect.com
SciVerse ScienceDirect
www.elsevier.com/locate/ijcip



Enhancing the security of aircraft surveillance in the next generation air traffic control system

Cindy Finke, Jonathan Butts, Robert Mills, Michael Grimaila*

Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA

ARTICLE INFO

Article history:
Received 28 December 2012
Accepted 15 February 2013
Available online 20 February 2013

Keywords:
Air traffic control
ADS-B
NextGen
Format-preserving encryption
FFX algorithm

ABSTRACT

The U.S. air traffic control system is reliant on legacy systems that artificially limit air traffic capacity. With the demand for air transportation increasing each year, the U.S. Federal Aviation Administration has introduced the Next Generation (NextGen) upgrade to modernize the air traffic control system. Automatic Dependent Surveillance-Broadcast (ADS-B), a key component of the NextGen upgrade, enables an aircraft to generate and broadcast digital messages that contain the GPS coordinates of aircraft. The incorporation of ADS-B is intended to provide enhanced accuracy and efficiency of surveillance as well as aircraft safety. The open design of the system, however, introduces some security concerns. This paper evaluates the limitations of the legacy systems currently used in air traffic control and explores the feasibility of employing format-preserving encryption, specifically the FFX algorithm, in the ADS-B environment. The ability of the algorithm to confuse and diffuse predictable message input is examined using message entropy as a metric. Based on the analysis, recommendations are provided that highlight areas which should be examined for inclusion in the ADS-B upgrade plan.

Published by Elsevier B.V.

1. Introduction

Despite the economic turmoil in the United States and abroad, air travel and transportation have only seen modest drops in activity. The most recent U.S. Federal Aviation Administration (FAA) report [1] notes that civil aviation contributes $1.3 trillion annually to the national economy, earning upward of $397 billion or about 5.2% of the gross domestic product. The aviation industry generated more than 10 million jobs in 2009 alone and in excess of 730 million passengers utilized air travel in 2011. Additionally, 26 cargo-only carriers operate within the nation's airspace to transport freight and mail; UPS announced that its aircraft hauled an average of 2.2 million packages in 2012 [20]. The United States is so heavily reliant on the air transport industry that the Department of Homeland Security has identified aviation as a key component of the transportation critical infrastructure sector.

With the constant demand for faster travel and package delivery, the volume of air traffic is expected to increase considerably. In 2011, air traffic control centers handled 41.2 million aircraft, and this number is expected to increase by 50% over the next 20 years, significantly stressing the air traffic control system [7]. For reasons of efficiency and cost savings, flights are expected to bypass the established airline hubs around which the air traffic network is currently structured. The resulting concerns about air traffic safety have provided the impetus to adapt the air traffic network and upgrade legacy air traffic control systems under the Next Generation (NextGen) plan.

The proposed changes include the upgrade to the Automatic Dependent Surveillance-Broadcast (ADS-B) system. The upgrade, however, introduces potential network-wide vulnerabilities. This paper assesses the current state of the air traffic control system, identifies the security risks

*Corresponding author.
E-mail address: jonathan.butts@afit.edu (J. Butts).

1874-5482/$ - see front matter Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.ijcip.2013.02.001

inherent in the ADS-B upgrade and evaluates a security solution designed to provide confidentiality for aircraft surveillance activities.

2. Background

The current air traffic control system is antiquated and is in need of an upgrade to meet the expected growth and safety considerations. This section evaluates the current state of the air traffic control system and discusses the FAA's NextGen plan and the associated vulnerabilities.

2.1. Air traffic control

The national airspace system is a complex system-of-systems designed to monitor and control the U.S. airspace. Aircraft typically fly predefined routes called "airways" that are designed to connect heavy traffic regions as efficiently as possible, while ensuring adequate radar coverage for monitoring traffic. Prior to takeoff, an aircraft is assigned a route comprising specific airways to follow to its destination. The route is updated as necessary during flight to avoid hazardous weather or congestion.

Presently, air traffic controllers monitor radar displays and provide positive control over the movement of aircraft to ensure safe separation. When an air traffic controller detects a potential conflict, navigational direction is provided to aircraft crews to restore safe separation. The directions and clearances are given via voice transmission over line-of-sight radio channels.

Although the air traffic control system operates in a satisfactory manner, it is by no means optimal and will be unable to accommodate the expected growth. Aircraft tracking and identification rely on outdated and unreliable surveillance radars. Indeed, primary and secondary surveillance radar have been the primary means of tracking aircraft since the late 1940s; the last significant air traffic control upgrade occurred in the 1970s [14]. Additionally, restricting flights to pre-determined airways is inefficient and imposes limitations on the density of air traffic.

Air traffic controllers depend on restricted communications to disseminate control messages. Frequent transmissions can potentially saturate the control frequencies. In busy sectors, controllers use multiple frequencies to receive concurrent communications from multiple aircraft, but such multitasking is constrained by human limitations. Human controllers are also subject to natural limitations (e.g., fatigue and information overload) and are susceptible to errors. As a result of these deficiencies, separation standards require artificial safety margins that, in turn, limit air traffic capacity.

2.2. NextGen security concerns

To overcome the aforementioned limitations, the FAA has introduced the NextGen upgrade [6], a comprehensive strategy to overhaul the air traffic control system. The strategy includes transformational programs for data communications, collaborative air traffic management technologies, and network-enabled weather information.

One of the most significant changes is the inclusion of the ADS-B system. ADS-B enhances surveillance capabilities and nearly eliminates the need for voice communications. Once it is fully implemented, the ADS-B system will enable the inclusion of more automated control systems, reducing the impact of human error and optimizing aircraft safety margins and efficiency [6].

The concept of automatic dependent surveillance (ADS) was introduced in the 1980s. The International Civil Aviation Organization has proposed the use of ADS technology in the future air navigation system (FANS) [4], which is focused on improving the communications, navigation and surveillance techniques employed in air traffic management. The vision includes improved navigation techniques using accurate satellite-based technology (i.e., GPS) and enhanced surveillance achieved by downlinking satellite-derived positions.

The term "automatic" in ADS means that pilot action is not required, "dependent" refers to the reliance on GPS technology to derive aircraft position and "surveillance" denotes the primary intended functionality [10]. ADS messages consist of data fields that specify information about aircraft position (i.e., latitude, longitude and altitude) and identification (i.e., aircraft-specific call sign). These messages are transmitted by aircraft at random intervals averaging two messages per second [15].

Message transmissions may be monitored by any receiver within range—there is no message confidentiality. The FAA has mandated that all air traffic be ADS-B compliant by 2020; this would enable any party—authorized or not—to monitor, with precision, the location of air traffic [6]. The lack of message confidentiality on the part of the ADS-B system has raised concerns among military, law enforcement and homeland security entities, all of which have secrecy and operational security requirements, but have to operate within the FAA-controlled airspace. Imagine the potential security risks of having Air Force One having to announce its exact location to any and all listeners.

The use of plain text (i.e., unencrypted) broadcasts enables ADS-B messages to be replicated. Recent research has demonstrated that it is possible to create and broadcast false messages with relative ease using inexpensive equipment [3,12,19]. Consider a scenario in which an aircraft controller's display shows a host of ghost aircraft—at best, this would create confusion and costly delays; at worst, it could lead to aircraft accidents [14]. In response to recent ADS-B hacker demonstrations (see, e.g., [3,19]), the FAA claims to have developed a comprehensive security action plan. However, the pertinent details of the plan are security sensitive and have not been released to the public [8].

Incorporating message encryption schemes could reduce the likelihood of false message broadcasts, ameliorate the resulting controller confusion, and assist in systemwide authentication. Additionally, message confidentiality would prevent aircraft surveillance by unauthorized entities.

2.3. Related work

Little research has focused on ADS-B security and, specifically, ADS-B message encryption. Samuelson et al. [21] have proposed techniques for enhancing the overall security of