Biometric Access to Training Devices as a Security Protocol in Flight Training

Brian Dillman[1,a,*], Renee Hendricks[1,b], Michael Petrelli[2], Stephen Elliott[2,c]

[1]Purdue University, 1401 Aviation Drive, West Lafayette, IN. 47907, USA

[2]Purdue University, 401 N. Grant Street, West Lafayette, IN. 47907, USA

ABSTRACT

Mechanical locks and keys are conventional access control devices utilized for both flight training devices and training aircraft, but keys can be copied, locks can be bypassed, and in the case of electronic flight training devices, unqualified instructors or students may utilize the equipment, possibly causing the equipment to fail. The faculty in the Aviation Technology Department at Purdue University performed this study to determine if biometric usage is a feasible and secure method in operating a flight training device and eventually securing an actual aircraft versus the older lock and key method. A Finger-vein biometric reader was installed onto a Frasca Advanced Aviation Training Device (AATD) and the software was installed such that identification had to be made prior to the program being able to initialize. The data collected from the survey includes information such as user interface issues and conditions which affect the failure reads such the placement of the flight instructor's finger on the biometric device.

KEYWORDS: Aviation Security, Security Threats, Biometrics, Biometrics Access Control, Finger-vein Reader, Flight Training Devices, Flight Simulation Devices

---

[a] Professor Brian Dillman is an Associate Professor in the Aviation Technology Department at Purdue University. With an academic background in aviation flight technology, he has extensive global experience in aviation safety to include Safety Management Systems. He has conducted multiple seminars in Taiwan and China and has published several articles on Aviation Safety within high risk environments.

*Corresponding author. E-mail: dillman@purdue.edu, phone: +1(0) 765 4949978

[b] Renee Hendricks was an Assistant Professor at Purdue University in the Aviation Technology department. Her research and teaching focus was in aircraft electrical systems, avionics systems, and aviation security. Renee has since returned to the industry as the Biometrics QPL lead for the Transportation Security Administration.

[c] Dr. Stephen Elliott is an Associate Professor and Director of the Biometrics Standards, Performance, and Assurance Laboratory in the Department of Industrial Technology at Purdue University. Dr. Elliott is also involved in national and international standards in biometrics, and serves as Vice Chair of INCITS M1 US biometric standards committee. Dr. Elliott is also Assistant Department Head of Industrial Technology, and a University Faculty Scholar.

1. INTRODUCTION

There needs to be a balance between necessary security protocols and flight instructor and student access to various training devices that are utilized in flight training. Up to this point, the usage of mechanical locks and keys has been a primary boundary to access both flight training devices and training aircraft. Even with a key sign-out protocol or dispatch office in place there are still areas where security can be breached and unwanted access can be obtained. Keys can be copied, locks can be bypassed, and in the case of electronic flight training devices (i.e. Frasca Advanced Aviation Training Devices, AATD), unqualified instructors or students may utilize the equipment for fun or in order to determine how it works, thereby causing unnecessary wear and tear.

2. LITERATURE REVIEW

2.1 AVIATION SECURITY

Security in the aviation industry has been based on three basic premises; positive identification and screening of passengers, screening of baggage, and verification that both passengers and baggage each board the aircraft. There have also been a variety of processes established to determine whether or not a particular individual poses a threat to an aircraft on a particular flight with varying degrees of success. In addition to passenger screening and identification, screening of baggage has evolved to the point where everyone and everything is screened at various levels prior to boarding an aircraft. Finally, only individuals that have a boarding pass and government issued ID are allowed beyond a security checkpoint which reduces the possibility of a "safe" individual checking-in and then handing the boarding pass to someone with a harmful intent. While these security protocols work for the commercial airline industry and are supported by government agencies and funding, they do not exist for corporate aircraft, the charter industry, general aviation airports or even flight training facilities. Individuals with the financial means to acquire a corporate aircraft do so to save travel time and forgo the security processes. Furthermore, typical passengers on corporate aircraft are well known to everyone involved from the scheduling deputy to the line crew to the pilots and the successful outcome of the flight is seldom in doubt. In many instances there is no need to determine whether or not an individual poses a threat to the aircraft since it would be obvious if a "non-approved" individual tried to gain access. The intent of this literature review is to

illustrate many of the specific security protocols used for commercial aviation, to highlight the potential government mandates that are being considered for business size aircraft and to create a testing platform to identify processes which can be adopted or modified for commercial and corporate aircraft, the charter industry and even for the general aviation airports and training locations.

2.2 POTENTIAL SECURITY THREATS

Various agencies have identified multiple types of security threats from different entities and individuals. As reported by Paul Proctor (1987) in “Corporate Concerns About Terrorism Spurs Sales of Security Systems”, the National Business Aircraft Association suggests operators with aircraft security systems should use them at every destination, no matter how brief the stay, because "it doesn't take very long for a bomb to be placed or a hydraulic line to be cut." While this type of security threat is to be considered, there are low cost alternatives typically available such as security fencing, restricted access to ramps, and watchful personnel on the airport ramp. Acquisition of an aircraft and the potential usage of it for harmful purposes is another matter. Although the extent of potential damage from light, corporate, and training aircraft is debatable, there is a real possibility that these aircraft are being targeted for terrorist activity. Eric Lichtblau (2005), in his report on US aviation security holes, refers to a government report which detailed particular vulnerabilities in what it called "the largely unregulated" area of general aviation, which includes corporate jets, private planes and other unscheduled aircraft. Mr. Lichtblau (2005) also references a previously undisclosed 24-page special assessment on aviation security by the Federal Bureau of Investigation and the Department of Homeland Security which indicates that Al Qaeda may have discussed plans to hijack chartered planes, helicopters and other general aviation aircraft for attacks because they are less well-guarded than commercial airliners.

2.3 PASSENGER AND BAGGAGE SECURITY SCREENING SYSTEMS

The US government has started many nationwide programs to determine whether or not an individual poses a threat to an aircraft. The most current program being highlighted for commercial aviation is the registered traveler program. Mark Prismon and David Johnston

(2004) quantify the main initiative underlying the program as to allow frequent fliers to volunteer for a criminal background check in exchange for a shorter security process at the airport. Mr. Prismon and Mr. Johnston (2004) also say that the program will require a fingerprint and iris scan to be taken at security stations to confirm identities. As of today there are only a select number of airports that are utilizing this program with various levels of success. There have been other systems before the registered traveler program. The Computer Assisted Passenger Prescreening Program (CAPPS) was one of the first screening programs initiated and implemented. The idea behind the CAPPS program was that by checking each passenger's address, name, phone number and date of birth, the airline could verify that the passenger was who they claimed (Wall Street Journal). In 2003 the newly formed Transportation Security Agency (TSA), which had previously been part of the Department of Transportation, set out to create a new version of CAPPS, popularly termed 'CAPPS II', and as initially proposed, CAPPS II was to be the transportation security equivalent of the credit report or mortgage score (Curry, 2004). Data about the individuals from their Passenger Name Records (PNR) would be linked with data available both publicly and in government files computing a score, and using the most sophisticated of statistical tools, passengers would be categorized as green, orange, or red, as trustworthy, perhaps questionable, untrustworthy, or even treacherous (Curry, 2004). This assessment of risk would then be utilized to allow access to an aircraft or increase the level of security necessary before a passenger is allowed to board. This of course assumes that the airline or commercial operator has a protocol established to handle individuals that are a perceived risk. In actuality one of the largest problems facing the CAPPS II program regards the action the airlines would undergo when finding a suspicious traveler (Prismon & Johnston, 2004). According to Mr. Prismon and Mr. Johnston (2004), in many cases, the airlines did not report the match to the government and in other cases the airlines did not properly remove the person from flying. This lack of reporting and response is contrary to the designed intent of the CAPPS II program.

In response to long waiting lines for airport security screening, the "Trusted Traveler" and "Registered Traveler" programs were introduced. According to the US General Accounting Office (GAO), many stakeholders believe that the Registered Traveler program will enable the Transportation Security Administration (TSA) to more efficiently use its limited resources by "more cost-effectively focusing its equipment and personnel needs to better meet its security

goals" (US General Accounting Office, 2002). The Registered Traveler program contains Personal information that can include any of the following: full name, current home address, current home phone number, current cell phone number, social security number, date of birth, place of birth, nationality, gender, prior home addresses, arrival date in US, digital photo, biometric reference, unique identification record number, Registered Traveler eligibility status, and information provided by Federal, State, and local government agencies and foreign governments that is necessary to carry out a security evaluation (Walters, 2004). The Registered Traveler program has been presented and promoted as a time savings option for airport security that shifts a portion of the operations cost to those individuals that choose to utilize the program. There is a registration and yearly operation fee that becomes worthwhile if an individual does extensive amounts of travel. On the other hand, for those individuals that travel sporadically or during relatively low travel periods the Registered Traveler program has not shown to save security screening time. There are individuals and groups that are less than excited and somewhat skeptical about the Registered Traveler program. Privacy advocates have raised concerns about possible data that may be included on the card in the future, and see the potential that when registering for the program the government can potentially check one's past criminal records (Prismon & Johnston, 2004).

Also, the need for tracking baggage and matching it to passengers has created a trend to shift from workload intensive barcode scanning technology to Radio Frequency Identification (RFID) on luggage. RFID technologies can assist in identifying exactly which baggage is in which container, match the baggage to the passengers and even provide an 'aboard aircraft' status, as well as exactly locate the container which holds the passenger baggage, all of which is invaluable from both security and operational efficiency standpoints (Cerino & Walsh, 2000). An RFID tracking system will allow baggage sorters to quickly identify a bag if it must be removed from an aircraft in the event a passenger fails to board an airplane or did not even pass the security checkpoint.

2.4 CORPORATE AIRCRAFT SECURITY

While commercial aircraft security is focused around the identification of passengers, an assessment of the perceived risk of those passengers, and positive matching of passenger

manifests to loaded baggage, corporate aviation security can be maintained by simply assessing the perceived risk of the passengers. While the amount of collateral damage caused by destroying a commercial aircraft in flight is significant, the potential impact of destroying a corporate aircraft in flight is significantly diminished. Destroying a corporate aircraft in flight is counterproductive for terrorist activity and there are much more attractive ways of utilizing a corporate aircraft to cause damage.

Security for corporate aircraft has centered on increased vigilance for the reduction of possible security breaches and increased regulation by government agencies. The National Business Aircraft Association (NBAA) has expressed concerns about potential regulations from various government agencies. On the NBAA website they state, "The Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) are reviewing new security protocols for general aviation (GA) - What can the industry do to reduce its exposure to threats and maximize the flexibility required for operational missions?" The current concern centers around additional regulations for international flights that were proposed by the FAA on September 18, 2007 in a Notice of Proposed Rule Making (NPRM) document. Currently any aircraft that enters US airspace on an international flight must make prior notification of the time, place of entry, and the number of individuals on board the aircraft. The proposed rule would require flight crewmembers to compare the passenger manifest information with the information on the Department of Homeland Security approved travel document presented by each individual attempting to travel onboard the aircraft to ensure that the manifest information is correct, that the travel document appears to be valid for travel to the United States, and the traveler is the person to whom the travel document was issued. Without access to the appropriate equipment and databases, this places an undue burden on the flight crew. Furthermore, unlike commercial aviation where the security stations are in a fixed location, corporate security locations must be as mobile as the aircraft themselves so that the flexibility of operating a corporate or charter aircraft is not sacrificed.

2.5 FLIGHT TRAINING FACILITIES SECURITY

Many universities and local airports have flight simulators and training devices housed at their flight training facilities. Flight trainers and simulators are utilized for educating future and even

current pilots on flight maneuvers, methods, and processes. These items are of high value and contain important information regarding airports and flight paths and they, too, need to be secured at all times. Many of instructors at these flight facilities train future and current pilots on security awareness, but securing these facilities requires more than security awareness training of the employees and students. Many of the training facilities are open to the public during the week and have little or no access control limitations. If the public can access the facilities, then, there is a high possibility that they can also access the flight simulators, too, even though they are unauthorized to do so. It has even been said that the 9-11 hijackers, who flew and crashed the commercial airplanes into the World Trade Center, even trained at local flight schools. Not only would access control devices have prevented these individuals from entering these premises in an unauthorized fashion, but if these flight school employees had access to a security-type database, they may have been able to check their backgrounds and delayed the education process for them.

2.6 SHORT TERM SECURITY SOLUTIONS

An appropriate response to security threats is not always cut and dry. There are many factors and variables that need to be considered. Like any problem, the most simple and tangible actions are taken first while specific programs are evaluated for later deployment. Security Directive 96-05, issued in August 1996, declared that, "all passengers who appear to be 18 years of age will present a government issued picture ID, or two other forms of ID, at least one of which must be issued by a government authority" (Curry, 2004). While the requirement to present a government issued photo ID is a positive and necessary step, the overall increase in security relies heavily on the ability of individuals to make quick assessments as to whether or not the individual presenting the government issued picture ID is in fact the person they claim. Combine that with the fact that many Government IDs can be counterfeited and this is only a stepping stone to a complete system. Mr. Curry illustrates the directive, and like systems before, as tending to rely on the coherence of a person's identity - Is this person the one whom he claims to be? If the airline employee believes so, then the terms of the regulation have been met (Curry, 2004).

If there is a perceived threat then an obvious step to strengthen security is to increase the number of trained security professionals overseeing operations with increased risk. In response to potential threats, federal officials now say they have taken a number of steps to tighten security for helicopters, chartered flights and the like, as they did previously in temporarily ordering federal security guards and tougher screening for helicopter tours in the New York City area (Lichtblau, 2005). Quick and effective responses to specific threats are vital to the overall security net around the world. However, each security protocol that is established takes significant manpower to staff, burdens the flight operation, and eventually must be shifted to higher risk, higher priority areas to respond to more recent threats. The US government wants the same level of security on corporate and charter aircraft that they desire on commercial aircraft while individuals that utilize corporate and charter companies want the same freedoms they have come to enjoy with the significant costs that they support. These two ideals can be achieved with the proper planning and security devices and thorough evaluation. There must be a system established that will allow minimally trained individuals with a significant degree of investment and culpability to access data, assess the perceived risk, and make informed decisions as to whether or not to continue an operation or secure additional input.

2.7 BIOMETRICS AND BIOMETRIC DEVICES

Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity (2008). Biometric modalities can include traits such as the hands (hand geometry), fingerprints, iris, veins, voice and even keystroke dynamics from a computer keyboard. These biometric traits are used as a means for authentication by various biometric device readers. A human characteristic can be used for biometrics in terms of the following parameters:

- **Universality** each person should have the characteristic
- **Uniqueness** is how well the biometric separates individually from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** is the ease of acquisition for measurement.
- **Performance** accuracy, speed, and robustness of technology used.
- **Acceptability** degree of approval of a technology (Jain, 2004)

There are a variety of biometric modalities, none of which are a solution to all threats or risks. Given that the majority of biometric devices were available at Purdue University, from the Biometric Standards, Performance and Assurance Lab, an evaluation of modalities was undertaken. Some of the modalities were limited, due to the need to interact with the operating system but not impact the operation of the Frasca. Therefore single sign on software was needed, and this limited the biometric modality choice to fingerprint, finger-vein, and face. The team decided on finger-vein, as it was a relatively new biometric modality and suited the needs outlined by the group. Being that the hand vein ranked Medium (M) for all six parameters, the researchers at Purdue preferred such a biometric, but only had access to a finger-vein reader, which works similar to the hand vein reader. A commercially available finger-vein device was chosen for this study. One of the advantages for selecting this device was that it was compact in size and could easily be placed near the flight simulator computer. To operate, near-infrared light is transmitted through the finger and partially absorbed by hemoglobin in the veins. The device then captures and extracts this information to match against a previously stored template. All of the individuals were enrolled into the system, and subsequently identified each time they needed to access the flight simulator computer.

3. METHODOLOGY

The Federal Aviation Administration (FAA) would require extensive testing and approval before allowing a biometric device to be installed in an actual aircraft, so the Frasca Advanced Aviation Training Device (AATD) at Purdue University was utilized for this research project. Because of the extensive time and paperwork necessary to install a biometric reader in an actual aircraft, the AATD is an easier and more controlled platform from which data can be obtained and modifications can be made during the test period. The Aviation Technology Department at Purdue University acquired this new Flight Training Mentor Device, which has the latest technology of avionics for general aviation aircraft, in the Spring of 2007. The avionics package consists of the Garmin G1000, which is an all-glass avionics model. The Hitachi H1 Logical Access finger-vein reader was installed onto the Frasca Advanced Aviation Training Device (AATD) in the Fall of 2008. The biometric reader software was installed such that identification had to be made prior to the Frasca AATD software program was able to initialize. This allowed

only designated Purdue flight instructors to turn on and off the flight training device, increasing its security.

Before the flight instructors were able to utilize the biometric, they first had to be enrolled into the biometric software. To do so, the researchers asked each flight instructor to place their finger of choice onto the finger-vein reader. A template of the finger-vein pattern is stored, and subsequently used for identification at a later date. The enrollment process only takes a few seconds per individual, resulting in 60 flight instructors to be enrolled. - The research team then briefly discussed the reader's operation with the flight instructors as a group. The biometric software program was also setup so that the flight instructor would first input a standard instructor password (same for all instructors) and then have the finger-vein scanned for the computer system login. If both the password and finger-vein scanning matched the biometrics database, then the software program for the flight simulator would start and the devices on the simulator would also light up.

4. RESULTS AND DISCUSSION

The objective of this research project was to test a commercially available finger-vein reader, integrated with the computer login of a Frasca flight trainer, to test its effectiveness as an access control device as well as determine its feasibility of use. Installing the biometric reader on the flight trainer did indeed prevent unauthorized individuals from powering the trainer on. If the incorrect password was inputted, the flight instructors were unable to power up or operate the flight trainer. Also, if the incorrect finger (but the correct password) was placed on the biometric reader, the person would not be able to access the simulator. If the flight instructors did not place their finger properly on the reader, they, too, were unable to access the trainer. In addition, 20 additional students, not enrolled in the biometric software, were asked to place their finger on the biometric reader, and each time, the biometric software displayed a failure note and the simulator never powered on. The researchers were also able to view the biometrics login log to see all the failed attempts to access the system. General performance characteristics, such as a Receiver Operating Characteristic curve was not calculated at this time. There were no failures to enroll on this device.

The previous method of preventing unauthorized access to the training devices was only limiting access to the simulators after 5pm, when the department officially closed. Once the normal hours of operations cease, the exterior doors of the simulator building are locked and the only access into the building is with a key or a code. The flaw in the punch-code entry door is that the code has remained the same since the door was installed four years ago and the number is common knowledge among many faculty, students, staff and airport employees. During the normal work hours of 8am to 5pm, the students, faculty, flight instructors and anyone at the airport can access the flight trainers because there are no preventative measures to overcome in order to gain access to the training devices. The simulator building doors are unlocked and the interior door to the simulator room is also unlocked. Once access has been gained through the doors of the building, the Flight Training Devices can be turned on by anyone who chooses to turn on power to the computers.

In order to understand the user's acceptance of the finger-vein reader, the flight instructors were asked to voluntarily participate in an online survey. This allowed the researchers to gather data from the participants and at the same time allow the participants to remain anonymous in their answers. Of the 60 flight instructors, 43 replied to the online survey, giving a 72% return rate. These flight instructors also ranged in age from 19 – 25 years old, with an approximate mean of 21.5 years. The actual survey can be seen in Appendix A. In the survey, the flight instructors were asked to rate the overall ease in using the finger-vein reader, using five ratings. Of the 43 respondents, 19 selected 'Very Easy', 17 selected 'Somewhat Easy', 5 selected 'Somewhat Difficult' and 2 selected 'No Response'. In addition, the 5th rating 'Very Difficult' was not selected by anyone. From these selections, one can determine that over three-fourths (84%) of the respondents selected one of the 'Easy' choices. This indicates that there was a positive response to the addition of the finger-vein reader and it did not negatively impact the usage of the flight training device.

In the survey, the flight instructors were also asked to choose from 4 choices, based on their usage, if there was a learning curve associated with the biometric device. Of the 43 respondents, 19 selected 'No Learning Curve', 21 selected 'Slight Learning Curve', 1 selected 'Large Learning Curve' and 2 selected 'No Response'. From these selections, one can determine that most (93%), of the respondents selected one of the 'No or Slight Learning Curve' choices.

This highly positive response rate indicates that the addition of a finger-vein reader is mostly intuitive as to its use and most users were habituated in a very short time. Deployment and training costs are something that needs to be considered when deploying a biometric system. These results are very positive with respect to user habituation.

The flight instructors were also asked to choose from 4 choices, based on their usage, which access control method they preferred for the simulator application. Of the 43 respondents, 1 selected 'Lock and Key', 13 selected 'Username and Password', 27 selected 'Biometric', and 2 selected 'No Response'. From these selections, one can determine that over half (63%), of the respondents selected 'Biometrics' as a preferred method for simulator access control. Another 30% selected 'Username and Password', of which the password was also utilized along with the biometric scanning. It may have been worthwhile for the researchers to also provide the choice of 'Biometric and Password' to determine if those who chose the 'Username and Password option also preferred the biometric device. From these 3 sets of answers, the researchers then concluded that installing a biometric was indeed feasible for the simulator since many of the survey respondents felt the biometric was easy to use, did not require a large learning curve to use, and also preferred biometrics as the choice for access control for the simulator.

5. CONCLUSION

There are many facets to aviation security. As illustrated in the literature review there have been extensive efforts to identify the potential threat of passengers. Extensive measures are taken for each commercial flight to ensure that only those individuals for whom the sole purpose is for traveling from one location to another board the aircraft. Pilots and crewmembers are screened at the security checkpoints as well, but there have not been sufficient measures taken to prevent an unauthorized individual from gaining access to an aircraft while it is sitting on the ramp. Just like the cockpit of an aircraft, flight simulators also need to be limited to authorized and qualified individuals only. This research study determined that installing a biometric reader onto a flight simulator was indeed effective as an access control device and also feasible to use. Through the use of the survey and in the opinion of the respondents the addition of the biometric reader did not reduce the usability of the device. It added a level of security that had not been present in the past and allowed the individuals

responsible for the care of the flight training device to access the usage log to determine date and time of use in addition to which flight instructor accessed the machine. This not only added security but increased accountability for those utilizing the machine in case something needed to be repaired. Overall the addition of the biometric reader was a significant success and it offered tremendous insight into the potential problems associated with installing such a device on an actual aircraft. The researchers plan to next test other biometric devices on actual commercial and cargo size aircraft as well as continue testing biometrics devices on the remaining simulators in the building. The goal of the researchers is to have a biometric on every simulator and training aircraft utilized by the Aviation Technology Department at Purdue University. Another change the researchers would like to try for future studies would be to survey a wide spectrum of pilots, since the mean flight instructor age of this study was 21.5 years of age. While this is the mean age of instructors in the flight program at Purdue University, this is not the mean age of flight instructors or pilots currently in the aviation industry.

REFERENCES

- Cerino, A. and Walsh, P. (2000), Research and Application of Radio Frequency Identification (RFID) Technology to Enhance Aviation Security, *FAA Aviation Security R&D Division*, AAR-510
- Curry, M. (2004). The Profiler's Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation, *Surveillance & Society* 1(4): 475-499.
- Department of Homeland Security, (2007), Bureau of Customs and Border Protection. 19 CFR Part 122, Advance Information on Private Aircraft Arriving and Departing the United States; Proposed Rule, *Federal Register* / Vol. 72, No. 180.
- Jain, A. K. (28-30 April 2004), Biometric Recognition: How Do I Know Who You Are?, Signal Processing and Communications Applications Conference, 2004. *Proceedings of the IEEE* 12th: 3 - 5.
- Lichtblau, M. (2005), New York Times, *Government Report on U.S. Aviation Warns of Security Holes,* National Business Aircraft Association, Retrieved on March 13, 2008, http://web.nbaa.org/public/news/insider/security-0807.php.

- Proctor, P. (1987), Corporate Concern About Terrorism Spurs Sales of Security Systems, *Aviation Week & Space Technology*, p. 80.
- Prismon, M., Johnston, D. (2004), Airline Industry Security", *Chapter within Technology and Privacy in the New Millennium,* Ethica Publishing, Boulder, CO. Purdue University, Retrieved on May 4, 2008, http://www.biotown.purdue.edu/ecorpus/index.asp