3625 Alleghany Drive
Salem, VA 24153
1-800-675-7558
www.medeco.com

Airport Access Control and Tracking, and the Aviation and Transportation Security Act

November 12, 2008

By Jennifer Riley
Medeco High Security Locks

Abstract

The Transportation Security Administration (TSA), an administration of the Department of Transportation, is charged with protecting the nation's transportation systems to ensure the freedom of movement for people and commerce.[1] TSA employs more than 50,000 people focused specifically on the security of the nation's highways, ports, buses, mass transit systems and airports.

A key element of securing the national aviation system – one of the nation's most important transportation systems – is centered around controlling physical access at the nation's airports.

This paper will examine in more detail the access control issue, discuss the risks inherent in traditional security measures designed to protect airports, and offer specific security solutions to control and track access.

Introduction

The Aviation and Transportation Security Act, passed in November, 2001, following the September 11th tragedies, created TSA to "improve aviation security, and for other purposes."[2] As such, security at the nation's 450 airports is an important focus of the organization's enforcement and prevention efforts.

While the aviation industry is undoubtedly a global enterprise, a key element of aviation security begins at the local level through controlling, tracking and analyzing individuals' access and attempted access to every airport's numerous secure areas.

Individuals who are responsible for managing airport security should familiarize themselves with the Act's security recommendations and requirements – several of which specifically address the issue of access – as well as previous incidents involving unauthorized access or attempted access at aviation facilities and the potential for future security threats.

Section 106 – "Improved Airport Perimeter Access Security"

The Aviation and Transportation Security Act covers a wide variety of issues and concerns related to transportation security, from the deployment of federal air marshals to improved flight deck integrity measures. Included in the Act, and of interest particularly for purposes of this discussion, is Section 106 of the Act, "Improved Airport Perimeter Access Security." [3]

Section 106 focuses in large part on strengthening and improving access control at airports, in part by deploying personnel in secure areas of the airport to control access and protect an airport's physical assets, but also by employing security technology that helps manage access control. Some of the Act's specific language in discussing access control includes the following:

- "The Under Secretary may provide for… technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport.''[4]
- on an ongoing basis, assess and test for compliance with access control requirements, report annually findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found;

(amends Section 44903(g)(2) of title 49 of the United States code – a compilation of the United States' general and permanent federal law.

- work with airport operators to strengthen access control points in secured areas (including air traffic control operations areas, maintenance areas, crew lounges, baggage handling areas, concessions, and catering delivery areas) to ensure the security of passengers and aircraft.

Additionally, Section 106 of the Act is further supported by National Security Presidential Directive 47 (NSPD 47), Homeland Security Presidential Directive 16 which details, in part "a strategic vision for aviation security while recognizing ongoing efforts, and directs the production of a National Strategy for Aviation Security and supporting plans."[5]

NSPD 47 suggests employing a layered security approach to monitoring and controlling access to the nation's critical aviation infrastructure to increase security without impeding the flow of people and goods. Specifically, the Directive recommends public and private sector cooperation toward improving security by, "sharing threat information; conducting prudent risk assessments; working to implement essential upgrades; and investing in protective measures such as staff identification and credentialing, access control, and physical security of fixed sites."[6]

The Directive further cites that the protective measures considered are to include "new and emerging technologies" and that an airport's multiple access points and secure areas must be included in the layered security approach.[7]

Unauthorized Access – A Real and Recurring Problem

TSA's and The Aviation and Transportation Security Act's focus on controlling airport access isn't based on a perceived need but rather on well-documented, widespread and ongoing threats to airport security through real-life incidents of security breaches.

Consider some of the following recent examples of unauthorized airport access:

- Just before midnight on July 4, 2008, a motorcyclist gained access to the Del Rio, Texas, airport's runways. The motorcyclist proceeded to drive on the runways at a high rate of speed without lights before abandoning the motorcycle and fleeing on foot. The airport director theorized that the motorcyclist gained access to the runways because he had the access codes to one of five keypads at that airport that open security gates to vehicular traffic.[8]
- U.S. Immigration and Customs Enforcement (ICE) officials arrested 20 workers at Chicago's O'Hare International Airport for obtaining and using fraudulent airport security badges that gave the workers unauthorized access to some of the airport's most sensitive, secure areas, including the tarmac. An officer and manager of the temporary agency that employed the workers were also arrested, and according to criminal complains unsealed in the case, more than 100 workers possessed the airport security badges obtained through fraudulent measures.[9]

  In discussing the case, Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, said, "If we are to ensure public safety, we must know who has access to the secure areas of airports. A fundamental component of airport safety is preventing the use of false identification badges, and punishing those who commit or enable such violations."

- At the United Kingdom's Heathrow Airport, four Greenpeace activists breached airport security and gained access to the tarmac. They then hung a banner on a British Airways Airbus A320 to protest the airport's planned expansion.[10]
- 17 U.S. airports, including Chicago's Dulles and O'Hare, Atlanta, Phoenix, and San Antonio, were forced to make emergency changes to their facilities' keypad codes that control access to secure areas of each airport, including planes and the tarmac, after a Mesa Airlines employee misplaced his laptop containing security information, including access codes, for those airports.[11]

Airport security breaches, particularly those involving fraudulent use of keypad code and airport employee badges to gain access, are a serious threat to the security of the nation's transportation systems, so much so that the TSA is working with aviation industry associations, including the Airports Council International – North America (ACI-NA) and the American Association of Airport Executives to address the issue of airport security breaches by employees.

Security breaches can often times be traced to the locking hardware as well as to the end user. For example, fraudulent use of keypad codes doesn't indicate a failure of the technology, but rather of the end user sharing the access codes, either purposefully or inadvertently, with unauthorized users.

Similarly, unauthorized access using a fraudulently copied key is the result of a failure of both the security hardware as well as the authorized key holder. Keys that don't utilize patented anti-copying measures cannot be considered as providing the high security that airports demand. Similarly, an authorized key couldn't be copied were it not for some failure on the end user's part either to protect that key from falling into the wrong hands or to ensure that he or she didn't provide copies to unauthorized users.

Airport security breaches can often be traced to a technology or human failure, or some combination of the two.

In commenting for an article in *Airport Business* magazine about the O'Hare security breach, Bob Cammaroto, TSA's acting general manager of the transportation sector network management – commercial airports, acknowledged that incidents such as the one at O'Hare "illustrate the concerns that arise around employee access control and badging."[12]

In the same article, Charles Chambers, senior vice president of security and facilitation at ACI-NA, said, "There's always a high level of concern about employee badging and screening and incidents do occasionally occur."

Badges and keypads, while prevalent security measures employed by airports to control access, are unfortunately not the only security systems subject to being breached in order to gain unauthorized access to a facility and its assets.

Traditional Security Systems and Why They Are Inadequate

Electronic security systems utilizing security cards, badges, or alpha numeric codes increase convenience at the expense of security. These types of systems particularly when compared to traditional mechanical lock and key systems that don't utilize patented key control, are accompanied by a specific and unique set of drawbacks inluding:

- Many popular on-door electronic security systems do not provide audit information which is critical to access accountability
- Most electronic systems are not suitable for use on perimeter gates of secure areas
- Expense to install, both from a time and materials standpoint
- Installation locations dependent on the availability of power and network lines
- Installation requires significant modifications to the door or frame, or both, increasing cost and decreasing portability
- Using a keypad generally does not provide information on who entered the code since codes can so easily be shared

Similarly, mechanical locks are prevalent throughout airports, and understandably so, as an important line of defense for controlling access to certain areas of the facilities and for protecting property. They're quick, easy, and inexpensive to install. There's a certain comfort level associated with this familiar security system used countless times daily to protect homes, vehicles, offices and other valuables. They don't require users to memorize access codes or carry electronic access cards, and traditional locks are, cosmetically, unobtrusive. Unfortunately, most locks are also woefully inadequate when it comes to protecting an airport and the nation's aviation transportation system since many popular systems are not protected against unauthorized duplication of the credential and they cannot provide audit information nor specific scheduling of personnel.

The traditional lock and key system is a good solution in situations where there is only one person using the key, where tracking access isn't important, and where the need to add or delete keys from a system isn't a concern. But even this "one user, one key" situation, while fairly uncommon in today's environment, is fraught with risk. What happens if the key is lost or stolen, or worse yet, copied without the owner's knowledge?

This risk of unauthorized duplication, however, can be mitigated to a degree by using a high-security mechanical system. Often employing patented or otherwise restricted keys and locks that are extremely difficult to bypass, these high-security mechanical systems do offer a significant level of protection and control as compared to standard systems, albeit without an audit and tracking feature.

With that said, a traditional mechanical masterkey system, particularly one that isn't defined as high-security, simply doesn't offer the level of protection, flexibility and data needed to control access at airports. Masterkey systems are also out of compliance to what is recommended in the Act because they don't positively identify the employee accessing the secure area and they don't enable airport security management to assess and test for compliance with access control requirements.

When compared with other security options, traditional, non-high security mechanical masterkey systems present other inherent risks and weaknesses to airport security, including:

- No ability to track who is accessing or attempting to access a door, how often, and when.
- No ability to quickly add or delete keys from a system when a key is lost, stolen, or an employee is no longer part of the organization.
- Unpatented or otherwise restricted keys can be copied and locks easily bypassed without leaving physical evidence to serve as an indicator of a security breach.

- Users need multiple keys to access different locks.

By themselves, neither an electronic security system nor a masterkey mechanical system is the appropriate solution for airport access control.

Solutions

Section 106 of The Aviation and Transportation Security Act focuses in large part on strengthening and improving access control at airports, and encourages the investigation and implementation of new and emerging security technology that identifies who is accessing or attempting to access a secure area, and that tracks access and access attempts.

A viable, cost-effective solution to fullfilling these recommendations put forth by the Act lies in combining the best attributes and features of mechanical and electronic door locking systems.

Medeco High Security Locks designed and introduced Logic – a new electromechanical product line that consists of digital lock cylinders and digital keys – as an answer to security and access tracking needs by using the most desirable characteristics that both mechanical and electronic sytems offer.

Logic offers functionality similar to that of sophisticated electronic security systems, including audit trails, scheduling and the ability to add and delete users easily, but installs without any wiring, door or frame modifications or additional hardware and is available in padlocks and other portable formats.

Logic's digital cylinder and digital key look much like a traditional lock and key. The key is virtually indistinguishable from most car keys, with the exception of a small display screen, as is the cylinder. The difference lies in the digital technology contained in both the battery-powered key and the cylinder, which is powered by the key.

Logic's digital cylinder retrofits into existing hardware, enabling the replacement of an existing cylinder and mechanical key with the electro-mechanical Logic cylinder in less than five minutes. This upgrade results in a stronger mechanical system, and the ability to both electronically audit access and change accessibility features, such as times and authorized users, quickly.

With Logic, any key can be quickly programmed to work or not work on any cylinder, without being limited by a mechanical hierarchy like on a mechanical masterkeying system.

Knowing who is accessing or attempting to access facilities is a critical element in protecting the airport facilities and equipment. Logic systems allow up to 1,000 audit records to be pulled from the cylinder, with redundant 100 audit records available from the key, both showing who is entering the protected area, how often, and when, thanks to time and date stamps. This data enables administrators to regularly evaluate and assert that the internal controls are operating efficiently, and helps airport management comply with TSA's recommendation to assess and test for compliance with access control requirements and report those assessment findings annually.

Lost keys can simply be electronically deleted from the system to maintain security. And, any time a new user key is needed, it can be quickly and easily added.

Additionally, unauthorized key copying is removed from the equation because replacement keys are cut and issued only by the Medeco factory and because of the patented electronic technology in Medeco keys – two features that, combined, offer superior protection against unauthorized key copying.

Instant rekeying is another Logic benefit as keys and cylinders can be instantly and easily deactivated or reprogrammed with different access permissions or schedules, either by Medeco dealers or by end-users who choose to self manage their systems with an optional programming device and software.

While Logic's auditing and tracking features that show who is accessing or attempting to access a facility's secure areas and its technology that prevents unauthorized access are compelling by themselves, the installation benefits and portability shouldn't be overlooked.

Traditional electronic security systems, including card readers, biometric systems, or keypads, usually require electricity in order to operate, and if the system is being installed as a retrofit, significant installation expense in both time and materials. Logic cylinders simply retrofit existing mechanical cylinders and leverage the use of existing door or fence hardware without any door or hardware modifications. No electricity, hardwiring, phone, or Internet connection is necessary. And, unlike many stand-alone systems, Logic cylinders blend discretely into existing hardware and architectural designs and are available in most common architectural finishes. In the event that security needs change, Logic cylinders can be easily moved to new doors, or when used in padlock applications, can be used virtually anywhere and in any environmental condition.

Logic provides a straightforward, cost-effective security solution where a mechanical masterkey system simply does not offer enough flexibility to keep up with airports' ever increasing security demands, and the ever-changing methods individuals are employing to gain unauthorized access to aviation facilities and equipment.

Logic offers strong physical security with the flexibility of schedules, audit trails, the ability to easily add and delete user keys, and unlike electronic systems, a retrofit cylinder that blends unobtrusively into existing hardware.

Conclusion

Threats to airports aren't going to disappear, nor are the regulations designed to protect them and the traveling public. In today's environment, aviation security isn't a question of whether protection is needed, but rather what type of protection is the best choice. The added complexities of ensuring compliance with TSA guidelines addressing access control and tracking make that security decision even murkier.

Both mechanical and electronics-only locking systems have their limitations when it comes to securing airports and providing the data and control needed to comply with governmental regulations.

A viable, cost-effect solution is a security system that combines the best attributes of both the mechanical and electronic systems and that can be deployed in any of the diverse applications within an airport facility .

For more information, please contact Joseph Kingma, Director of Business Development at Medeco High Security Locks: 1-800-675-7558 ext. 1683 or jkingma@medeco.com

References

1. www.tsa.gov

2. www.tsa.gov

3. http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf

4. http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf

5. http://www.dhs.gov/xprevprot/laws/gc_1173113497603.shtm

6. http://www.dhs.gov/xlibrary/assets/laws_hspd_aviation_security.pdf

7. http://www.dhs.gov/xlibrary/assets/laws_hspd_aviation_security.pdf

8. Southwest Texas Live!, Bill Sontag, "Fourth of July Airport Security Breach Begs Question: How Did This Happen?", July 13, 2008.

9. U.S. Immigration and Customs Enforcement, News Release, "ICE Investigation Leads to the Arrest of 23 Workers with Unauthorized Access at O'Hare Airport", November 7, 2007

10. www.liveleak.com/view?I=e05_1203969383, "heathrow Airport Security Breach", February 25, 2008.

11. WJLA-TV, "Pilot's Missing Laptop Causes Airport Security Scare", www.wjla.com/news/stories/0408/514346.html, April 24, 2008.

12. directory M Articles, http://articles.directorym.net/ACCESS_CONTROL_AND_BADGING-a878350.html, Anna Stanley, Assistant Editor, Airport Business.