



Moving About in Airports with Biometric Scanning

The World at Your Fingertips

BY CAMILLE SHIEH

Advanced technologies such as biometrics-credentialing kiosks are not just seen in movies; they are gradually appearing in high-risk settings such as at airport customs. Not only do biometrics help screen travelers, they are also exceptional management tools in safeguarding restricted areas and keeping tabs on attendance and payroll records.

Biometrics have not been popular in airport settings until recent years, as a result of the technical barriers that hindered their performance in real-life situations. Often, a biometric reader that performed perfectly in a laboratory test is less impressive in real life, as various environmental and hygienic factors obstruct accurate scans.

In the case of fingerprint scanning,

most optical sensors are configured to look for the presence or absence of total internal reflectance (TIR), which is the phenomenon whereby the interface between glass and air acts as a mirror at certain angles, said Phil Scarfo, Senior VP of Worldwide Sales and Marketing, Lumidigm. "The contact between the skin and the platen defeats the TIR, allowing those points of contact between the finger and the sensor to be imaged. Thus, those points of contact must be complete and visible to enable the conventional sensor to collect a fingerprint image. Optical and electronic sensors simply cannot do this time after time. All too often, 3 to 20 percent of the time, the reader is unable to detect the fingerprint."

In recent years, multispectral imaging technology has solved the fingerprint-capturing problems that conventional imaging systems encounter in less-than-ideal conditions. "This solution is based on using multiple spectra of light and advanced polarization techniques to extract unique fingerprint characteristics from both the surface and subsurface of the skin," Scarfo said.

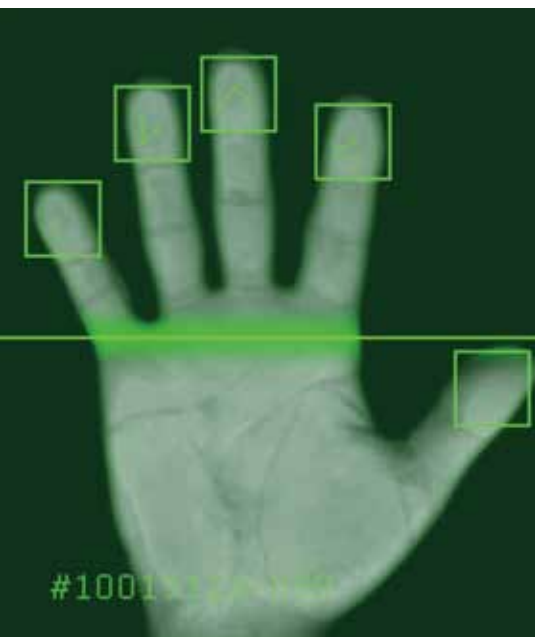
As airlines and airports work to

balance traveler convenience with the need for security, they will increasingly integrate advanced biometrics-based identity authentication technologies into the growing range of self-service processes within air travel, such as passenger and baggage check-in kiosks, said Scott Basham, Location, Perimeter and Surveillance Security Asia-Pacific Program Lead, Unisys. "This is because self-service processes have extended deeper into the air travel cycle — from online flight reservations to today's passenger and luggage check-in kiosks at domestic airports just prior to boarding a flight."

STAFF AND CREW MANAGEMENT

In "Recommended Security Guidelines for Airport Planning, Design and Construction" revised by the US Transportation Security Administration in May, while the use of biometrics is not a federal requirement for US airports, the higher degree of security is recommended for strategically significant facilities or high-risk portals.

Commonly used access control features that tie in with time and



▲ Multispectral imaging technology allows fingerprint capturing to be more precise than conventional systems, leading to growing popularity in airport security use.



Phil Scarfo, Senior VP of Worldwide Sales and Marketing, Lumidigm



Scott Basham, Location, Perimeter and Surveillance Security Asia-Pacific Program Lead, Unisys



Scott Mahnken, VP of Marketing, Bio-Key International



Mark Moscinski, VP of Safety and Security, System Development Integration



John Diedam, VP of International Sales, Ingersoll Rand Security Technologies



Aluisio Figueiredo, COO of Intelligent Security Systems

attendance and payroll involve a dual-authentication process, which includes a smart card with a photo ID and biometrics, said Scott Mahnken, VP of Marketing, Bio-Key International. "Depending on the life cycle of the access control system installed, incorporating time and attendance into access control is a logical step in the upgrading/replacement process," said Mark Moscinski, VP of Safety and Security, System Development Integration.

Restricting access for aviation staff can be easily configured by applying biometrics credentialing to sensitive entry points. For unsupervised access to high risk areas, biometrics clearly offer a more secure solution, Basham said. "But care must be taken to ensure that the biometrics cannot be circumvented — either through biometric spoofing or tailgating, where multiple people enter at the same time without verifying their separate identities."

"At Yeager Airport in West Virginia, hand geometry readers have been used since 2001, restricting access to the control tower located in the airport terminal and also to the HVAC system and other sensitive equipment," said John Diedam, VP of International Sales, Ingersoll Rand Security Technologies. "The control tower doors are opened about every five minutes around the clock. The

hand readers are all networked to the airport's central security system."

Staff's time-and-attendance records can be simplified as well. "Biometrics are often at the front end for time-and-attendance systems in all types of industries, including transportation venues," Diedam said. "Contrary to using badges, sign-ins or other ways of tracking employees, a biometric reader assures that no employee can punch in for another, eliminating time fraud and reducing payroll costs. This is why so many organizations now employ biometrics; for instance, at the Miami International Airport, the hand punch terminals take time and attendance even for janitorial services."

Eliminating "buddy punching" is only part of the reason that many want to upgrade, Scarfo observed. "Biometric time-and-attendance systems also prove to be more cost-effective in the long run. Within three to five years, biometric solutions become break-even with plastic cards because of the associated costs with cartridge and printer replacements, as well as the support and management of the system."

"We've received many requests for facial-recognition technology for airport employees," said Aluisio Figueiredo, COO of Intelligent Security Systems. "The main factor is that it is not as intrusive as iris and

fingerprint scanning. However, the drawback is that equipment setup must be in accordance with the environment; cameras must be placed in specific areas under specified lighting to ensure accurate readings. This technology cannot be set up just anywhere." The technology can be installed in both large- and small-scale airports, as it is affordable and can be implemented according to various planning needs and available budgets.

DANGERS SCREENED OUT

For external screening of travelers coming into or leaving the country, biometric scanning does provide double prevention against possible security breaches. In some airports, a database of collected personal biometrics data is integrated and connected to government databases for quick referencing and tracking of suspicious persons. "The database can be connected to a similar installment, such as the FBI's identification system, or it can be maintained independently in the cloud," Mahnken said.

Since 2002 in Europe, internal and external security systems in many European airports have already been interfaced with government databases to ensure air travel safety, said Arjan Bouter, International Sales Manager, Nedap Security Management. 



Security Management Taking Off

SUBMITTED BY
UTC FIRE & SECURITY, CEM SYSTEMS,
SYSTEM DEVELOPMENT INTEGRATION AND
BOSCH SECURITY SYSTEMS

Airport projects — both new and expansions/upgrades — are taking place all over the globe. These projects aim at putting integration-friendly systems in place for total security and safety management at major air travel hubs.

ZURICH AIRPORT MONITORED BY UTC FIRE & SECURITY

Unique (airport operator) operates Switzerland's renowned traffic hub, the Zurich Airport, and is responsible for the airport's daily management. The airport houses around 180 different companies. Unique employs approximately 1,400 people, and together with more than 260 airport partners, the combined total roughly equals 21,000 employees.

The Zurich Airport needed to upgrade its aging video surveillance system, for which obtaining replacement parts was often very difficult. Furthermore, the system could not be expanded, but scalability was demanded along with the expansion of the airport.

UTC Fire & Security offered a combined solution that integrates the existing 330 analog cameras by using 46 digital encoders. The encoders digitalize the camera data so that it can be transferred to the monitoring stations. Each monitoring station is equipped with 40 TB of local storage space, storing more than 400 million images, and events can be saved to the central storage (800 GB) when and if necessary. To avoid the costs associated with establishing a new network, the existing IP network was

used to transfer all data.

An additional advantage of the system is that it easily allows for future expansions. With UTC Fire & Security's system installed, Unique is able to monitor all events on its premises and, thus offers a safe environment to those passing through the Zurich Airport.

CEM SYSTEMS REFINES ACCESS TO HKIA

Hong King International Airport (HKIA) has about 900 aircraft movements, serves more than 160 worldwide destinations daily, and had more than 50 million passengers in 2010 pass through the airport, making it one of the busiest international passenger airports.

In 2010, HKIA awarded CEM Systems (a Tyco International Company) a US\$2-million security management system upgrade contract. The HKIA upgrade was significant as more than 1,000 serial readers were seamlessly upgraded from Wiegand technology to PicoPass smart-card technology using existing IP connectivity at the airport for simplified installation.

The contract also included a further expansion of fingerprint card readers to all air bridges. The progressive move to biometric card readers was achieved to increase the overall

efficiency of the airport.

The fingerprint readers increase HKIA's security by providing three levels of identity checks, including ID authentication, PIN check and fingerprint verification. Each reader has a large internal database which holds card and encrypted biometric templates at the door. This ensures zero system downtime at air bridges. The reader also features an LCD to show personnel meaningful user messages and has many airport-specific door modes such as "Passenger Mode" and "Lobby Mode" for extended doors-open times at air bridges. With the readers in place, only authorized and trained personnel can use the air bridges.

HKIA also uses portable readers for mobile security. The reader allows security personnel to make roaming checks throughout the airport and can also be used at temporary entrances where there is no mains power. This ensures the highest level of security at all times.

SDI UPGRADES A MIDWEST AIRPORT'S ACCESS CONTROL

System Development Integration (SDI) was contracted by a US international airport in the Midwest to upgrade all hardware and infrastructure to support the



biometrics component of its access control system (ACS). The ACS controls the passage of staff (not passengers) into secure and sterile areas of the airport. In order for the ACS to be fully secure, the system must address three checks for an individual's identity: something s/he has (ID badge), something s/he knows (PIN) and something s/he is (fingerprints).

To minimize service disruption, three subprojects took place. The first challenge was to issue new smart-card ID badges containing unique biometric data to more than 45,000 active holders in a period of less than three months. During this process, every active badge holder was required to submit a new badge application, have his/her badge photo updated, and enroll in the system with two fingerprints that were subsequently stored on an encrypted smart card as a biometric template.

The second subproject targeted the installation and deployment of biometric card readers at each of the employee checkpoints in the airport in order to enhance employee screening. Biometric verification would now be required to allow employee access through each checkpoint. A new fiber-optic network and new control panels were installed throughout the airport as the badge enrolment process took place.

The third subproject focused on the biometric validation of badge

holders entering the airfield at a busy drive-in post. The post witnesses airfield access to between 6,000 and 7,000 vehicles per day. This high-traffic entrance screens not only airline employees, but contractors and other service personnel. With the implementation of wireless handheld biometric card readers, all access is now granted through validation of biometric information. A customized gate software application provides the security officer with instant visual verification that all people entering with vehicles are valid badge holders.

BOSCH SECURES BERLIN INTERNATIONAL

Bosch Security Systems was selected to install security and safety systems at the new Berlin Brandenburg International (BBI) airport. The scope of the order includes the planning and installation for the fire alarm system, electroacoustic emergency-warning system, emergency exit door controllers, intrusion detection system, video surveillance, access control and building functions.

BBI represents the most important infrastructure project in Germany's capital region and is Europe's largest airport construction site to date. It is built to better connect Berlin and the entire region with major destinations in Europe and throughout the world. Further, it will be an important contributor to the regional economy; BBI is expected to create up to 40,000 new jobs.

Optimal protection against fire hazards with around 19,000 automatic and manual fire alarms and a whole host of fire control systems will be installed. They will be connected to a total of nine networked UGM universal security systems. The networked public address (PA) and evacuation system with around 11,500 speakers is planned for passenger information and evacuation in the event of a hazardous situation. The PA and evacuation system will also be used for voice announcements for passenger information and for the gate-paging stations.

In addition, an intrusion detection system will be integrated with the fire, PA and evacuation systems. The information for surveillance is recorded using around 1,200 emergency call couplers. The video surveillance system consists of 300 network dome cameras, 260 HD video cameras as well as 900 video cameras of different types. It will be managed by the Bosch video management system. Bosch will also install more than 600 kilometers of copper cable for the fire alarm and intrusion detection systems as well as the electroacoustics.

The new BBI airport will most likely go into operation in June 2012. With 280,000 square meters of terminal and pier space, a baggage sorting hall of 20,000 square meters, as well as a 9,500-meter conveyor line, it will be one of the largest airports in the world.

