Little Rock National Airport

Using more sophisticated integrated designs, some enterprises now audit their facilities looking for special areas where security needs to be treated differently than in the overall plan. Often those special places get piggybacking technologies.

Government facilities and airports have pioneered the effort.

For example, Little Rock National Airport needed to protect restricted areas from unauthorized personnel. To do so, the airport set an ambitious goal: Deploy a combined smart card reader/ biometric fingerprint reader solution to ensure extremely tight control of movement within the facility and eliminate unauthorized entry.

Little Rock National Airport is the state's largest commercial service airport, handling more than 2.1 million passengers annually. It attracts passengers from a large part of Arkansas as well as a number of surrounding states. There are more than 150 airline flight arrivals and departures each day.

CASE SUMMARY

Location:
Little Rock, Arkansas

System:
Software House:
C•CURE 800

Airport security is not only responsible for the airport's own 150 employees, but also for airport tenants, who work for various airlines or in airport restaurants and gift shops. As one of the first airports to consider a dual card reader/biometric solution, they were breaking new ground. They developed an RFP with help from Garver Engineers, an Arkansas-based engineering firm, who hired security consultants Jim Brindle Associates to work out the technical specifications required for the 210,000 square foot facility.

Report and monitoring

Airport officials sought a solution that would seamlessly integrate biometric and smart card technology, and also enable future upgrades. This would provide multiple layers of security while preserving an easy-to-use system for airport personnel and card holders. Another key criterion was the ability to create custom reports and adjust how alarm activities were displayed on monitoring screens.

Airport officials chose security integrator Advent Systems Inc., which recommended both Software House and BioScrypt products. "These companies have great reputations," said Tim Doll, director of operations for the airport. "We found Software Houses' customers were very happy with them."

Based on the integrator's recommendation, the security officials replaced their outdated security system with a scalable security management solution encompassing complete access control, along with smart card and biometric fingerprint readers from BioScrypt. The integrators installed 110 readers controlling access to airport doors and vehicle gates.

The airport also installed a dedicated security backbone in the terminal, which included redundant servers to prevent loss of information in the case of a hardware failure. System redundancy was transparent to users; if the main server were to fail, service would be restored instantly via the backup server. Using separate standalone servers would prevent any unauthorized entry into the security system through the airport LAN.

Switching to a new security system in an airport is no easy task. The integrators were responsible for keeping the facility secure at all times, which required running both security systems concurrently until all aspects of the new system were fully tested. "This went along seamlessly," said Doll. "There were no hiccups at all … The products work great together."

Alarm lights on map

Before the system went live, the integrators trained airport personnel, including the operations director, security staff, badging clerks, dispatchers and maintenance staff. "Our users love the new system because they feel more secure," said Doll. "It has made our dispatchers' lives so much easier. Our previous system displayed coded text on the monitors, so dispatchers would have to know what each code meant for each alarm. [The new system] simply displays a map of the terminal building with a flashing light indicating the location of the door in alarm mode on the map, tells the dispatcher the reason for the alarm, such as 'door forced open' and shows a picture of the person using the door along with pertinent information about them."

Today, all new airport tenants, contractors and employees who require access to restricted areas provide a fingerprint and background investigation in order to receive a badge. The fingerprint is stored on the smart card, which also contains a specific security level that defines which doors and gates each person can access.

Whenever entering a secure area, the user presents his proximity smart card to the card reader, which flashes a green light indicating that the card contains authorized clearances and that he should proceed with the biometric verification. The user then places his finger on the fingerprint reader, which connects to the system's database to verify the user's authenticity.

If authenticity is confirmed, the door automatically opens. If the system identifies an unauthorized person seeking access, it automatically alerts the police and sends a report to the communications center, along with a photo of the person whose card is being used, key information about the user, and the reason for access denial, such as lost or stolen card. With the pertinent data and photo in hand, communications center dispatchers can instantly provide police with a description of the individual.

The airport has issued approximately 1,900 cards to date. Airport tenants are required to notify badging personnel immediately if someone is no longer in their employ so they can automatically disable the badge.

Idea spreads

"Today, the airport is more secure," said Doll. "We have better reporting capabilities. We have more control over monitoring and changing things on the system than we did before. I can sit at my desktop and change parameters on any door in the airport, pull up a report if someone left a door open and have information within seconds on who went through the door last. It's worked out great. I get four to five calls a month from other airports looking to do the same thing."

During the specification process, Doll kept the TSA apprised of the new security processes. The agency was pleased that the airport has eliminated the chance of someone using a lost badge to gain access, and is considering making this type of system mandatory for all airports.

The airport continues to enhance its security capabilities with plans to integrate all security systems to work with the new system. With these new stringent security measures in place, the airport offers passengers increased peace of mind during their travel to and from the region.