

Security Products

New Threats, New Arsenal

A wave of advanced technology changing the face of airport security

By Robert A. Hile Sep 01, 2010

When entering an airport, travelers can't help but reflect back on the events of Sept. 11, and how things have changed since then.

In recent years, travelers have gained the ability to check in for their flight online, change their seat and download an electronic boarding pass to a PDA. It's also possible to check the flight status from a PDA before leaving for the airport.

The rapid advancements in technology have enabled passengers to be more efficient and informed. But has airport security changed or evolved?

Security professionals recognize the advancements in security technology and innovations. The adoption of innovative solutions and even non-traditional security measures provides additional safety to the traveling public and lessens the chances that an act of terrorism could take place.

Advanced Imaging Technology

Technophiles may want to be screened by the new full-body scanners that are being used in most major airports today. These advanced imaging technologies are starting to gain wider acceptance in today's security-minded environment, but there are still a small, yet significant, percentage of the traveling public that feel these devices are invasive because they "see through" your clothing.

For this reason, TSA has implemented strict privacy safeguards designed to prevent the officer assisting the passenger from seeing the image and the officer viewing the image from seeing the passenger. All communication between the officers is conducted using wireless headsets to allow for seamless communication without violating passenger privacy.

In most cases, travelers still have to go through a metal detector before entering the full-body scanner. This equates to extra time being allocated to each passenger, restricting traffic flow. It also means an additional officer must be dedicated to that specific screening area. The good news is that the newer versions of these systems offer enhanced scanning technology so passengers only have to be checked by one method.

The IP Route

There also has been an evolution of IP in airport security programs. Virtually every major airport in the United States is upgrading or planning to upgrade its surveillance system. Analog CCTV systems are being upgraded or replaced with IP-ready technologies. Older video recording devices are being swapped out for network video recording packages that are capable of managing thousands of cameras.

Cost-effective digital storage arrays are being added to the overall system configuration to store recorded video for longer periods and make it readily available at a moments notice for forensic purposes. Video compression technology continues to improve with standards like H.264, which allows for more efficient transmission, distribution and storage of high-resolution video across the entire security network.

One of the great benefits of an IP camera is that these sensors can be deployed anywhere there is secure network access. In addition, more IP surveillance cameras are capable of being powered over the Ethernet, thus lowering the overall cost of installation by reducing infrastructure costs.

All of these technology advancements enable increased camera coverage of critically secure areas within an airport facility and the availability of high-resolution, recorded video immediately during an incident or breach.

The IP evolution also has been a major catalyst for improving the way airports protect the perimeter and operations areas. The traditional approach included separate systems like fencing, fiber-optic fence detectors, microwave beam detectors, ground-based radar and CCTV systems.

Often these systems operated on a stand-alone basis and were monitored separately. Today's advanced perimeter protection and intrusion detection packages often include a robust video analytic framework that uses an IP backbone to tie separate and disparate systems together under a single "layered" security platform. These types of configurations offer no single point of failure and are designed to allow different sensors to work together, offering the highest assurance of detection with minimal false alarms.

Getting Analytical

Video analytic packages today offer a wide range of capabilities such as "object left behind," which is used to detect a bag or package that has been left unattended.

Entry and exit monitoring detects when a person is traveling the wrong way through a pre-defined secure exit point.

Auto-tracking is an additional advancement in video analytics that is starting to show real promise in today's airport environment. This feature allows for proactive tracking of a suspicious person by manually identifying and virtually tracking the subject. Once initiated, the surveillance system will automatically track the suspect within the confines of the airport. This can be accomplished by clicking on the subject as he or she moves through a live camera view. The system will intuitively follow or track the person from one camera view to the next.

The same algorithm can be employed to use recorded and stored video in a forensic manner to quickly identify and efficiently locate a suspect in the event of breach. This is accomplished by marking the suspect and using pre-recorded video from multiple cameras on the network to track and locate the perpetrator within minutes, eliminating the need to shut down and clear an entire terminal.

This feature has the potential to save any airport a tremendous amount of time and money, which is a solid business-case justification for adding and implementing a new video analytic package. Once applied to a surveillance system, a properly designed and tuned video analytic package can add incredible electronic intelligence to any system, providing early and accurate detection.

Since Sept. 11, airports and other critical infrastructure organizations have been beefing up their physical security systems and sub-systems. Department of dedicated to that specific screening area. The good news is that the newer versions of these systems offer enhanced scanning technology so passengers only have to be checked by one method.

The IP Route

There also has been an evolution of IP in airport security programs. Virtually every major airport in the United States is upgrading or planning to upgrade its surveillance system. Analog CCTV systems are being upgraded or replaced with IP-ready technologies. Older video recording devices are being swapped out for network video recording packages that are capable of managing thousands of cameras.

Cost-effective digital storage arrays are being added to the overall system configuration to store recorded video for longer periods and make it readily available at a moments notice for forensic purposes. Video compression technology continues to improve with standards like H.264, which allows for more efficient transmission, distribution and storage of high-resolution video across the entire security network.

One of the great benefits of an IP camera is that these sensors can be deployed anywhere there is secure network access. In addition, more IP surveillance cameras are capable of being powered over the Ethernet, thus lowering the overall cost of installation by reducing infrastructure costs.

All of these technology advancements enable increased camera coverage of critically secure areas within an airport facility and the availability of high-resolution, recorded video immediately during an incident or breach.

The IP evolution also has been a major catalyst for improving the way airports protect the perimeter and operations areas. The traditional approach included separate systems like fencing, fiber-optic fence detectors, microwave beam detectors, ground-based radar and CCTV systems.

Often these systems operated on a stand-alone basis and were monitored separately. Today's advanced perimeter protection and intrusion detection packages often include a robust video analyti framework that uses an IP backbone to tie separate and disparate systems together under a single "layered" security platform. These types of configurations offer no single point of failure and are designed to allow different sensors to work together, offering the highest assurance of detection with minimal false alarms.

Getting Analytical

Video analytic packages today offer a wide range of capabilities such as "object left behind," which is used to detect a bag or package that has been left unattended. Entry and exit monitoring detects when a person is traveling the wrong way through a pre-defined secure exit point.

Auto-tracking is an additional advancements in video analytics that is starting to show real promise in today's airport environment. This feature allows for proactive tracking of a suspicious person by manually identifying and virtually tracking the subject. Once initiated, the surveillance system will automatically track the suspect within the confines of the airport. This can be accomplished by clicking on the subject as he or she moves through a live camera view. The system will intuitively follow or track the person from one camera view to the next.

The same algorithm can be employed to use recorded and stored video in a forensic manner to quickly identify and efficiently locate a suspect in the event of breach. This is accomplished by marking the suspect and using pre-recorded video from multiple cameras on the network to track and locate the perpetrator within minutes, eliminating the need to shut down and clear an entire terminal.

This feature has the potential to save any airport a tremendous amount of time and money, which is a solid business-case justification for adding and implementing a new video analytic package. Once applied to a surveillance system, a properly designed and tuned video analytic package can add incredible electronic intelligence to any system, providing early and accurate detection.

Since Sept. 11, airports and other critical infrastructure organizations have been beefing up their physical security systems and sub-systems. Department of Homeland Security grant funding and, most recently, American Recovery and Reinvestment Act stimulus dollars have driven the incredible growth and expansion of these systems. Hundreds of cameras are in place, leading to an information overload of sorts.

Officers and security operators can no longer effectively mine and manage the amount of security information being captured. The continued evolution and deployment of IP-ready products, coupled

with the need for real-time situational awareness, has led to the development of physical security information management systems. The value these software packages deliver to an organization is tremendous.

Total Awareness

The simple truth is that any physical security program can be made more effective by enabling different sensors and inputs to work with each other to provide total situational awareness of any possible threat situation. In addition, today's command and control systems have the ability to gather, compile and make information available from numerous non-related security sub-systems, such as graphical information systems, airport operations systems, flight operations systems, local and national crime databases, weather data, environmental control systems, fire and life safety systems, lighting systems and mass notification systems, and more. In a crisis, the availability of reliable, relevant and realtime data is vital to the overall success of any security program.

Imagine having the ability to seamlessly manage all key elements of any situation based on the electronic collaboration of all the earlier mentioned subsystems. This could include automatic tracking and dispatch of first responder and emergency forces, communication and data sharing between multiple agencies simultaneously, electronic enforcement of key emergency policies and procedures, electronic record keeping of any event and the ability to archive every aspect of any event for any predetermined time period. These systems are available today and are extremely effective in providing real-time detection and intelligence faster than any human could hope to achieve.

Most of these systems have software platforms that are designed for mission-critical environments, making them highly reliable and fail safe. When something tragic occurs and you need to respond now, you don't want to be in the middle of a software reboot or a failure of key functions.

A Closer Look

Any discussion of airport security today also should include a mention of a nontraditional security practice, referred to as behavioral screening. TSA has been criticized because its primary focus was on using technology alone to detect weapons or suspicious behavior. The group responded in 2003 by launching a program called Screening of Passengers by Observation Techniques.

Although highly controversial and specialized, numerous U.S. airports are using some form of behavioral screening to enhance security programs. One airport in particular, Miami International Airport, has trained more than 30,000 airport employees on how to detect anomalies in human behavior.

Lauren Stover, director of security and operations at Miami International Airport, is blazing a trail for airport security professionals by augmenting her traditional technology-based security program with behavioral screening.

"Ill intentions are not part of the DNA of someone's biometric profile," Stover said. "Our program provides a highly reliable layered approach to securing our facilities and protecting our customers. Having new technology that would help us enhance our behavior screening methodology would be a welcome addition to our overall security program."

Moving forward, the sky is the limit on the continued evolution of intelligent security technologies in airport environments. New and innovative products will be developed to assist security professionals with being proactive in addressing any perceived or relevant threat. Open standards like ONVIF, PSIA and OSIPS will drive the ease of integration between IP-enabled security devices.

Further development will be made on chemical, biological and radiological sensors. There will be innovation in and around the field of biometrics, which will help dual-level authentication become

common practice for entering or accessing secure airport flight and operation areas. Standards like TWIC will propel the adoption of a single-card credentialing system for all airport personnel.

“I think the biggest challenge that any customer is faced with is deciding which technology to choose,” said L. Clint Welch, manager of aviation security and public safety at San Diego County Regional Airport Authority. “For example, in the area of video surveillance, IP-based systems have become the great equalizer. With the advent of cheaper, higher-quality solutions, the small-scale user has access to many, if not all, of the same capabilities and features that were traditionally reserved for large-scale operations that could afford more complex and capable systems.”

About the Author

Robert A. Hile is the director and segment head of integrated security solutions at Siemens Building Technologies.

Copyright 2010 [1105 Media Inc.](#)