Kevin M. Panneton
Professor Stephen Saravara
Security Management 44.312.201
25 November 2009

Promising technologies to meet tomorrow's security challenges

Within the field of industrial and corporate security, a constant partnership between man and technology takes place on a daily basis in an attempt to mitigate security threats. In past years many forms of industry have found themselves thrust onto the stage of a global economy, bringing with it unforeseen and ever changing threats. In order to counter these new threats, the security industry and a vast array of service providers have devised new and innovative solutions to take on a proactive approach to counter security vulnerabilities through advancements and innovations in technology. From corporate offices to the theme parks and government facilities to our very homes, technology is transforming to meet the needs of both asset and personnel protection. Some of the most promising technological advances are still in the developmental phase or are in the process of field testing, but one thing is for sure, they are exceptionally sophisticated and will change the face of the security industry in the years to come. From automated explosive detection units and advanced millimeter wave and backscatter technology in our nation's airports to global positioning systems and biometric identification within government and corporate industry, a new era in corporate and industrial security is emerging.

The security industry has been developing technology for decades, but following the attacks of September 11, 2001, these advances have become an even more visible counter measure for many citizens that would normally not interact with such advanced security technology. One particular area where this advance has taken center stage is within our nation's transportation system, especially airports and other mass transit modes. To get a better idea of some of the newest systems that have been developed in recent years and put into real world service, all you have to do is take a flight.

The Transportation Safety Administration better known as the TSA, has put in place several systems which include the Rapiscan 620DV and Smiths Detection HI-SCAN 6040 aTIX x-ray machines, which are utilized to scan packages and personal luggage. The advanced Rapiscan 620DV utilizes both horizontal and vertical x-ray capabilities to give a complete perspective of items content regardless of its orientation within the machine and also has the ability to apply explosive detection software. The Smiths Detection HI-SCAN 6040 aTIX uses several independent multi-energy generators combined with advanced x-ray sensor technology to give real time analysis to the operator of any possible threats to include explosives. These advances not only enhance the operator's ability to get a full picture of the packages being processed, but it increases throughput, a key component for officers when dealing with weary travelers. Although currently in their test phase, the TSA has also begun to put in place several new promising systems that include millimeter wave and backscatter detection units. The Millimeter wave system utilizes revolving non-ionizing electromagnetic radio frequency energy within the advanced imaging spectrum, and computes the reflected energy as a three-dimensional image of the subject and any objects on their person. Backscatter technology is based on the same whole body principle, but uses low level X-ray to create a high resolution image much like that of millimeter wave systems. Although these machines have great potential within the security industry, they also have a fundamental flaw when it comes to personal liberties. Regardless of privacy concerns, these systems utilize advancements in technology that were once primarily engineered for medical purposes, but now have the potential to save lives in a very different way.

Another advance in technology that assists in operational security measures is the global positioning system. Although not a new concept, the possibilities when used in conjunction with advanced mapping and geographical applications could prove to be fundamental for the security industry. Originally designed for military purposes the global positioning system has proven it usefulness in a wide range of civilian applications. The systems currently available not only guide families back and forth from a weekend away, but are being utilized by managers and security personal to track the movement of both assets and vehicle fleets. Industrial security has taken on new roles in today's society with the continuous growth of a global market system and the many subdivisions corporations manage all over the globe.

Advances in the global positioning system could one day allow security managers to have real time oversight of all their personal and resources without having to physically track each and every asset. This capability could prove instrumental in loss prevention and overall security.

Although future improvements in package scanning and asset tracking may be an important focus to security experts, the most promising advances in technology that can aid the security industry are the continuing development of biometric systems.
In an article by David B McIntosh titled *Biometrics – a fad or the future* he states that "biometrics offer a unique new security feature, the ability automatically to double-check the identity token against the true identity of the individual using it to claim access." While many corporations utilize the identification card as their primary means of identification and access, stand alone I.D. cards pose a fatal flaw and can become a great security threat when they are inadvertently lost or stolen. With the implementation of biometrics even in its current state, security can be dramatically enhanced to protect against fraud and unauthorized access on all levels. Biometric identification is an automated approach to recognize individuals through either physiological and behavioral characteristics or a combination of both and can be used in conjunction with today's identification methods to enhance overall security. Unlike traditional methods such as radio frequency identification cards, pin numbers or passwords, biometrics offers a more secure way to positively identify an individual. This can be accomplished by scanning an individual's face, fingerprints, hand geometry, iris, and even voice recognition known as dynamic signature, to truly and systematically verify a person's identity. This technology can potentially prevent the security risk posed by credentials alone, by enhancing the overall identification process. Most typical systems are made up of several integrated components which include a sensor, signal processing algorithms, data storage, matching algorithm, and either a human or computer generated decision process. Although when described in technical terms the system seems complicated, in reality it utilizes the basic principles of geometry and pattern recognition. What was once a technology only seen in futuristic concepts is quickly becoming a growing reality in today's security industry.

According to an article in Biometric Technology Today, biometrics "growth will be caused by a range of global phenomena, which will require a level of authentication available only through the use of biometrics, these include the emerging central role of the digital identity in IT, population mobility and workforce decentralization, demand for eGovernment services, near ubiquitous reliance on digital transactions, and the inevitability of broadband access everywhere." Biometrics has great potential with further development, and will most likely be applied to a whole spectrum of services and security measures in the years to come.

The first and most common application of biometrics in use today is fingerprint recognition. This basic concept has been used by law enforcement agencies for decades but until recently was a manual and time consuming process. Fingerprint identification has since become the most widely used biometric process due to its ease of acquisition and longstanding history within the law enforcement and immigration services. Currently one of the main systemized finger print data base systems is managed by the Federal Bureau of Investigation and is known as IAFIS. The IAFIS system is designed to identify possible suspects by comparing an individual's fingerprints to those maintained within a computer data bank or manually by those stored on file. Although this technology is primarily used for investigative purposes, it also has great potential as an immediate form of positive identification for the security sector. Fingerprint recognition utilizes the distinct ridgeline patterns by identifying the direction and bifurcation of those lines that are unique to each individual. This can be accomplished by utilizing a variety of imagery and sensor systems which include thermal, ultrasound, capacitive, and the most commonly used optical. One good indicator that fingerprint recognition is a viable and cost effective security measure is that commercial use of this technology has increased throughout the years. It is now possible for smaller corporations and individual citizens to purchase these devices for use with anything from personal computer passwords to granting access into secured rooms in a small business setting. Finger print recognition technology is a tried and proven method for identification purposes, and its potential is nearly limitless with advancements in its application.

As one of the first successfully commercial tested biometric systems, the hand and finger geometry approach is also a practical solution to personal identification. This system is relatively simplistic, biometrically speaking, and can be used in conjunction with other verification techniques that are available. Much like a finger print scanner, this system relies on saved information within a computer data system to identify a match through a comparison process. Typically this starts with the person entering a personal pin number then placing their full hand onto a scan pad, where the computer system is designed to compare the measurement submitted by the applicant at an earlier date. The geometry of the individuals hand is then calculated and matched to the saved measurements on record, which allow or denies entrance into the requested area. Unlike credentials alone, both finger prints and hand geometry are nearly impervious to forgery by utilizing a more hands on approach to a personal identification.

Another biometric system in use today is the iris and retinal scan process. Iris recognition is a concept that dates back to the mid-nineteen hundreds, but truly was advanced in 1994 with the creation of an algorithm that could perform iris recognition automatically through the use of advanced software. This process is designed to analyze the distinct and random patterns of and individual's iris. The system first locates the iris by using landmark features and the distinctive shape of an individual's iris, which then allows a high resolution image to be taken for further analysis. Although many employees may be hesitant to use this technology in the future because of the misconception that the system uses laser technology, it actually utilizes infrared lighting and digital imagery that causes no harm or discomfort to the individual. The image taken is then computed to create a pictorial code that can be used to compare to the digital read out stored within a computer data base. In the future this system could prove instrumental in aiding with verification for anything from banking to high level security access.

As a relatively new concept, facial recognition is also becoming one of the frontrunners in the biometrics field. The principles behind facial recognition unknowingly happen on a daily basis with human interaction, but in the early nineteen-sixties an automated computer model was devised. This new technology has improved dramatically over the past decade with the advance in computer technology, and now in its current state can be used for both verification and identification purposes.

Facial recognition took center stage and proved its usefulness when it was used as a security measure during the 2001 Superbowl in Tampa Florida. This first widely publicized application was used to identify suspects by capturing images in rapid succession and automatically comparing that data with mug shots stored on a criminal database. The recognition process can be accomplished by analyzing either features based or geometric and photometric or view based. There are currently three main algorithms that support this function which include Principal Component, Linear Discriminant Analysis, and Elastic Bunch Graph matching. Principal Component Analysis is a technique pioneered in the late nineteen-eighties and along with Linear Discriminant Analysis offer two analytical forms of recognition. Elastic bunch graph matching has the greatest potential for future applications as it is not greatly influenced by variations in lighting, arbitrary in-depth rotations, or facial expressions. This technique is based on the concept that real face images can be transformed into a dynamic link architecture that can be computed onto an elastic grid. Although each technique has complications that can diminish their accuracy, a combination of all three algorithms is likely to prove as a viable solution in future applications. According to a report published by the National Science and Technology Council, "Through the determination and commitment of industry, government evaluations, and organized standard bodies, growth and progress will continue, raising the bar for face recognition technology." Facial recognition has great potential in the industrial security sector by aiding guards and managers with identifying possible threats when manpower may be understaffed or overwhelmed with the flow of human traffic within a facility.

Currently, many of these biometric systems are being utilized by high level government agencies and large corporate entities. However, as the technology improves and the cost decrease they are likely to become obtainable for use by a larger portion of the security industry. Future advancements in computer processing, biometric technology, and positive identification techniques will allow this current technology to become more efficient and user friendly. New innovations and advancements using the basic principles of identify individuals through unique human traits is likely to be a prevailing approach to meet the needs of the future security industry.

Although the above concepts have great potential to assist security experts, they are only a small component of the many breakthroughs that lay ahead. Future technological improvements in the industrial security field will not only come from advanced computer systems, data banks, software, and biometrics, but also from advancements in building hardening, emergency preparedness capabilities, and asset protection abroad. One of the unfortunate lessons learned from the World Trade Center attacks in 2001 and the ongoing pirate threat off the coast of Somalia is that the private sector is no less vulnerable to the threat of violence than that of government and military resources. It is a reality in today's corporate world that security experts must not only safeguard personnel and property simply from within the company facilities, but must also plan for unforeseen and unconventional threats against those assets both in the United States and abroad. While protecting physicals resources is an important role for industrial security experts, protecting human assets from conventional explosives, chemical, biological, and even nuclear weapons, must remain on the minds of security personnel today and into the future. Although the probability of these threats is less likely than many of the daily security issues that test corporations today, they must still be viewed as viable threats that require attention.

The industrial security sector now has the capability to take on these new threats through advancements that have been made and continue to be made in construction materials, engineering, medical technology, and less than lethal weaponry all of which can all be deployed to counter unconventional means of attack on corporate assets. Building hardening is a concept that has been utilized by the military and government agencies going back to the onset of the cold war era and beyond. With the emerging threats that we face as a society today, this same approach can be implemented to create a security envelope around corporate buildings and outpost by utilizing anything from simple concrete pillars to sophisticated shear wall designs for steel high-rise buildings and advanced air filtration units. Understanding the threats that exist can help security managers better mitigate a wide range of possible situations through the implementation of proper emergency planning and new advancements in technology. While building security and emergency preparedness are important proactive measures, in the unlikely scenario were the industrial sector must defend itself against imminent harm, new improvements in less than lethal weaponry can aid security personal.

Although the idea of proprietary or contract security officers having the ability to utilize weaponry may be a hard notion to accept, techniques such as electrical shock, chemical, impact projectile, physical restraint, light, and acoustic may be the future in corporate defensive measures and should not be overlooked. One of these breakthroughs in defensive weaponry is the Long Range Acoustic Device (LRAD) developed by the American Technology Corporation. This technology was developed originally for military applications, but shows great potential for use in the civilian sector as a tool for perimeter security and infrastructure protection. The LRAD system can be utilized for audio notification or as a crowd control measure with the capability to direct just over one hundred and fifty decibels with great accuracy. This system is now undergoing real world testing form the battlefields in Iraq and Afghanistan, to protecting luxury cruise lines and oil platforms from attack. Although their effectiveness is still debatable, the technology and engineering behind the system will likely pave the way for future less than lethal options.

While future advances in technology will allow the security industry to take on unforeseen challenges, it is also imperative to remember that human to human interaction will always be the greatest deterrent. Technology has its limitations; it does not have intuition nor an awareness of its surroundings, it does not understand human emotions or personalities, and most importantly it does not understand loss whether it be life or property. Nonetheless, taking into consideration the new challenges that face security personnel today, these technological advancements are imperative in aiding us to overcome biological limitations and weaknesses. Technology should never entirely replace the human element, but can assist us in the security industry by enhancing our natural human abilities. The challenges that the future hold are unknown and sometimes unimaginable, but with innovation and proper application, advancements in technology will undeniably change the face of industrial and corporate security.

Works Cited

Advanced Technology Checkpoint X-Ray
<http://www.tsa.gov/approach/tech/advanced_technology.shtm>

Biometrics Overview
<http://www.biometrics.gov/Documents/biooverview.pdf>

Biometric Technology Today; May2009, Vol. 17 Issue 5, p9-11, 3p

Biometric Technology Today, Volume 15, Issue 4, April 2007, Page 9

Face recognition across pose: A review.
Pattern Recognition; Nov2009, Vol. 42 Issue 11, p2876-2896, 21p

Imaging Technology
<http://www.tsa.gov/approach/tech/imaging_technology.shtm>