United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
2:00 EDT
Thursday,
April 25, 2002

NATIONAL PREPAREDNESS

Technologies to Secure Federal Buildings

Statement of Keith A. Rhodes
Chief Technologist

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
25APR2002	N/A	-

Title and Subtitle NATIONAL PREPAREDNESS: Technologies to Secure Federal Buildings	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office P.O. Box 37050 Washington, D.C. 20013	**Performing Organization Report Number** GAO-02-687t
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
Thank you for inviting me to participate in todays hearing on security technologies to protect federal facilities. The terrorist attacks of September 11 on the World Trade Center and the Pentagon have intensified concerns about the physical security of our federal buildings and the need to protect those who work in and visit these facilities. These concerns have been underscored by reports of long-standing vulnerabilities, including weak controls over building access. As you requested, today I will discuss commercially available security technologies that can be deployed to protect these facilities, ranging from turnstiles, to smart cards, to biometric systems. While many of these technologies can provide highly effective technical controls, the overall security of a federal building will hinge on establishing robust risk management processes and implementing the three integral concepts of a holistic security process: protection, detection, and reaction.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR

Number of Pages
72

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on security technologies to protect federal facilities. The terrorist attacks of September 11 on the World Trade Center and the Pentagon have intensified concerns about the physical security of our federal buildings and the need to protect those who work in and visit these facilities. These concerns have been underscored by reports of long-standing vulnerabilities, including weak controls over building access.

As you requested, today I will discuss commercially available security technologies that can be deployed to protect these facilities, ranging from turnstiles, to smart cards, to biometric systems. While many of these technologies can provide highly effective technical controls, the overall security of a federal building will hinge on establishing robust risk management processes and implementing the three integral concepts of a holistic security process: protection, detection, and reaction.

First I will provide an overview of the technologies that provide protection, detection, and reaction capabilities against the most prevalent threats. I will describe the characteristics and capabilities of each of these technologies and summarize their effectiveness, as well as their maturity and other performance factors to be considered in implementing them. While not endorsing any product, I will also identify vendors and costs. Finally, I will discuss the considerable technical challenges and user acceptance issues still ahead in their implementation.

In conducting our review, we interviewed officials at federal agencies responsible for the physical security of their buildings, including the General Service Administration's (GSA) Federal Protective Service, the Defense Protective Service, the U.S. Capitol Police, and GAO's own Office of Safety and Security. To understand the availability and effectiveness of newer security technologies, we also met with officials from GSA's General Products Center and technologists from the National Institute of Justice's Office of Science and Technology, the Department of Defense's (DoD) Biometrics Management Office, and the Biometrics Foundation. We coordinated with the Security Industry Association and its advisory councils that represent the different security industries within the scope of our work. They provided us with valuable information and contacts. We attended the Biometric Consortium Conference and the International Security Conference and Exposition, where newer technologies were demonstrated and where we discussed aspects of the technologies with industry representatives. We also discussed the results of several of the Federal Aviation Administration's biometric prototype initiatives with

program managers. To familiarize ourselves with available security products, we also conducted an extensive literature search and obtained and perused technical studies performed by independent organizations and compared their results with vendor-provided information. We selected the vendors listed in the attachments to this testimony based on factors such as market share, assessment studies, and availability of equipment on the GSA schedule. We obtained equipment prices from vendors and GSA schedules. Finally, we relied on previous GAO work on physical building security. We performed our audit work from February through April 2002 in accordance with generally accepted government auditing standards.

Background

It is the federal government's responsibility to assure the physical protection of its facilities and the safety of employees and visitors of those federal buildings. GSA, through its Public Building Service (PBS) is the primary property manager for the federal government, owning or leasing 39 percent of the federal government's office space. Approximately one million federal employees, millions of visitors, and thousands of children and their day-care providers enter these facilities each day. Within PBS, the Federal Protective Service is responsible for the security of most GSA-managed buildings.

Over thirty other executive branch agencies, including DoD and the departments of State, Veterans Affairs, and Transportation, have some level of authority to purchase, own, or lease office space or buildings. These agencies are responsible for the security of their own sites. The U.S. Secret Service is in charge of the security of the White House and other executive office buildings. The U.S. Capitol Police secures the Capitol complex, which includes the Capitol and House and Senate office buildings. The marshal of the Supreme Court and the Supreme Court Police tend to the security of the Supreme Court. Marshals from the Department of Justice's U.S. Marshals Service ensure the security of other federal courts.

Security Issues Have Been Reported at Federal Buildings

The 1995 domestic terrorist bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, aroused governmentwide concern about the physical security of federal buildings. One day after the bombing, then President Clinton directed Justice to assess the vulnerability of all federal office buildings in the United States, particularly to acts of terrorism and other forms of violence. Justice led a working group in developing a report that established governmentwide minimum

standards for security at all federal facilities.[1] Also in 1995, the president directed executive departments and agencies to upgrade the security of their facilities to the extent feasible based on the report's recommendations, giving GSA this responsibility for the buildings it controls. Among the minimum standards for buildings of a higher risk level specified by the Justice report are security technologies, including closed-circuit television (CCTV) surveillance cameras, intrusion detection systems with central monitoring capability, and metal detectors and x-ray machines to screen people and their belongings at entrances to federal buildings.

In June 1998, we testified on GSA's efforts to improve federal building security.[2] We reported that although GSA had made progress implementing security upgrades in its buildings, it did not have the valid data needed to assess the extent to which completed upgrades had helped to increase security or reduce vulnerability to the greatest threats to federal office buildings. We also expressed concerns about whether all GSA buildings had been evaluated for security needs. We recommended that GSA correct the data in its tracking and accounting systems, ensure that all GSA buildings were evaluated, and develop program goals, measures, and evaluations to better manage its security enhancement program. In October 1999 we again testified on GSA's efforts.[3] During this review, we found that the accuracy of GSA's security upgrade tracking system had improved and that almost all of its buildings had been evaluated for security needs.

However, a review we performed in April and May 2000 exposed a significant security vulnerability in the access controls at many government buildings.[4] Posing as law enforcement officers, we gained access to 18 federal facilities, where we reached the offices of 15 cabinet secretaries or agency heads. Our briefcases were not searched for weapons or explosives.

[1]The report, entitled *Vulnerability Assessment of Federal Facilities*, June 28, 1995, classified federal facilities into 5 security levels ranging from a level 1,with minimum security needs, to a level 5, with high security needs. Fifty-two increasingly stringent security standards were recommended, depending on the level of risk assigned to the building.

[2]U.S. General Accounting Office, *General Services Administration: Many Building Security Upgrades Made But Problems Have Hindered Program Implementation*, GAO/T-GGD-98-141 (June 4, 1998).

[3]U.S. General Accounting Office, *General Services Administration: Status of Efforts to Improve Management of Building Security Upgrade Program*, GAO/T-GGD/OSI-00-19 (Oct. 7, 1999).

[4]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (May 25, 2000).

As mentioned previously, last September's terrorist attacks against the World Trade Center and the Pentagon have focused even greater security concerns about federal buildings. Such concerns have prompted agency officials to create a more stringent security environment at their facilities. For example, the Federal Emergency Management Administration recently informed GSA officials that it was canceling plans to move its national headquarters and 1,000 workers to the Potomac Center redevelopment near the waterfront in Washington, D.C. Citing security concerns about the new building, the agency backed out of a 10-year lease.

Despite a show of increased security, it remains uncertain whether effective countermeasures have actually been implemented. For example, reporters who visited a number of government agencies in late October demonstrated that, without thorough screening, nonemployees could easily gain access to freely wander the buildings.

Since the 1995 Oklahoma City bombing, the federal government has already spent more than $1.2 billion on increased security measures for the federal government's office space. Following the September 11th terrorist attacks, increased resources have been appropriated for this purpose. Specifically, on September 18, 2001, President Bush signed the Fiscal Year 2001 Emergency Supplemental Appropriations Act (P.L. 107-38), appropriating $40 billion to respond to the terrorist attacks. The act provides funding to cover the physical protection of government facilities and employee security. On September 21, 2001, the president allocated $8.6 million from this appropriation to GSA's Federal Buildings Fund to provide increased security for federal buildings. On October 17, 2001, the president requested that Congress increase the total to $200.5 million for the Federal Building Fund for additional security services at federal buildings. The president's fiscal year 2003 budget requests that $367 million be made available from the Federal Building Fund to fund costs associated with implementing security improvements to federal buildings.

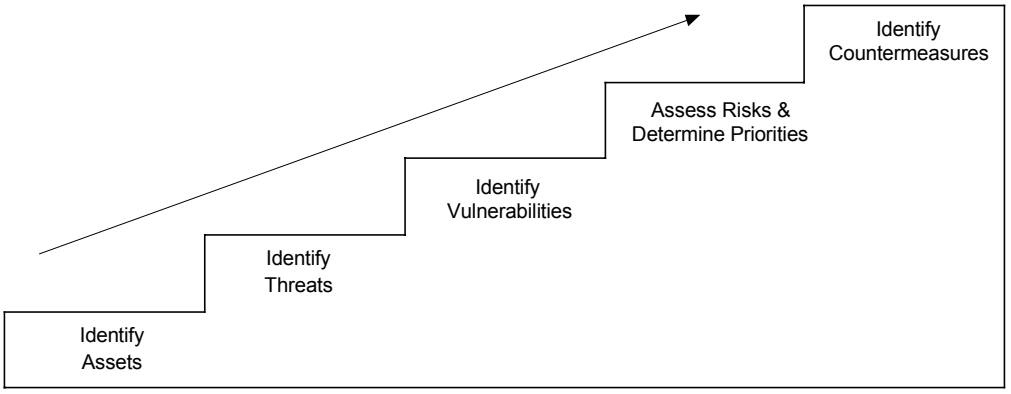
On March 21, 2002, the Bush administration asked Congress for an additional $27.1 billion in emergency funding for fiscal year 2002 for needs stemming from the September 11th terrorist attacks, $5.5 billion of which were for domestic security. Some of these requested funds will most likely be invested in technologies to enhance building security. It will be important to ensure that the technologies that these funds are spent on are effective.

Risk Management is the Foundation of Effective Security

The approach to good security is fundamentally similar regardless of the assets being protected. As GAO has previously reported for homeland security[5] and information systems security,[6] applying risk management principles can provide a sound foundation for effective security whether the assets are information, operations, people, or federal facilities. These principles, which have been followed by members of the intelligence and defense community for many years, can be reduced to five basic steps that help to determine responses to five essential questions.

Because of the vast differences in types of federal facilities and the variety of risks associated with each of them, there is obviously no single approach to security that will work ideally for all buildings. Therefore, following these basic risk management steps is fundamental to determining security priorities and implementing appropriate solutions.[7]

Figure 1: Five Steps in the Risk Management Process



Source: GAO.

[5] U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Oct. 31, 2001).

[6] U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68, (May 1998).

[7] GSA's building security upgrade program uses a risk assessment approach whereby threats and vulnerabilities are identified and corresponding security countermeasures are identified to either reduce or eliminate each threat and vulnerability.

What Am I Protecting?

The first step in risk management is to identify assets that must be protected and the impact of their potential loss. Included among the assets of federal facilities are the physical safety and peace of mind of the occupants, the value of the structure itself, and the importance of the mission of the organization housed in the facility. The symbolic value of certain landmark federal facilities and monuments must also be considered in the assessment.

Who Are My Adversaries?

The second step is to identify and characterize the threat to these assets. Is the threat, for example, that unauthorized individuals can gain access to the building to commit some crime, or that an authorized yet disgruntled employee intent on causing harm to fellow employees or the facility can get in, or, still more menacing, that a terrorist will introduce a chemical/biological agent or even a nuclear device into the building?

The intent and capability of an adversary are the principal criteria for establishing the degree of threat to these assets. The terrorist bombing of the World Trade Center in 1993, the Oklahoma City bombing of the Alfred P. Murrah Federal Building in 1995, the U.S. embassy bombings in Tanzania and Kenya in 1998, and last year's September 11th terrorist attacks on the Pentagon and the World Trade Center leave no doubt as to the existence of adversaries intent on causing the maximum harm. And, as these events have tragically demonstrated, our adversaries certainly have the capability. Moreover, more recent information gathered by intelligence and law enforcement agencies have led government officials to believe that both foreign and domestic terrorist groups continue to pose threats to the security of our nation's infrastructure, including our public buildings.

How Am I Vulnerable?

Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach? For a facility, weaknesses could include vulnerabilities in the physical layout of the building, its security systems, and processes. For example, the lack of a standoff distance between vehicle access and the building itself, which would allow an adversary to detonate a car or truck bomb within a dangerous distance of the building, is an example of a vulnerability in the perimeter security of a building. Or, it might be that an antiquated and labor-intensive access control system in combination with an inadequate security staff create

weaknesses in security systems and processes that allow entrance to a building.

What Are My Priorities?

In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss of or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities. For example, the risk of loss of human life due to poor access controls on weekends, when fewer people are working in the building, is lower than on weekdays during standard working hours.

What Can I Do?

The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

Many security technologies were developed in a research environment. However, in a real-world environment, some degree of security must be traded off against operational and safety considerations. Extreme security countermeasures cannot be implemented if they could disrupt operations or adversely affect the safety of the occupants of a building. For example, an access control system that uses draconian methods to screen employees at public entrances would be inappropriate except in buildings at the highest risk level because it would cause maximum inconvenience to large numbers of building occupants at peak traffic hours. Moreover, an access control system cannot be so rigid that it impedes the safe exit of a building's occupants during emergencies, such as a fire. In all cases, an acceptable balance between security and these competing factors must be reached, which can only be decided by the building's occupants.

Protection, Detection, and Reaction are Integral Security Concepts

Countermeasures identified through the risk management process support the three integral concepts of a holistic security program: protection, detection, and reaction. Protection provides countermeasures such as policies, procedures, and technical controls to defend against attacks on the assets being protected. Detection monitors for potential breakdowns in protective mechanisms that could result in security breaches. Reaction, which requires human involvement, responds to detected breaches to thwart attacks before damage can be done. Because absolute protection is impossible to achieve, a security program that does not also incorporate detection and reaction is incomplete.

To be effective, all three concepts must be elements of a cycle that work together continuously. To illustrate, suppose that the protection of a side door of a federal building is provided by a lock, which is wired to an intrusion detection sensor, which triggers an alarm to alert a guard to initiate a reaction. If someone picks the lock, thereby tripping an alarm, and a guard is monitoring the detection system in real time, she or he will detect the incident and can react to contain the intrusion and apprehend the intruder before damage is done. However, if no guard is monitoring the intrusion detection systems to react to the intrusion, the process breaks down and the security of the building may be compromised. In other words, technologies that implement the concepts of protection and detection cannot alone safeguard a building. An effective human reaction is essential to the security process.

Myriad Commercially Available Security Technologies Support Security Concepts

Myriad security technologies, at various stages of commercial development, support the security concepts of protection, detection, and reaction. We have categorized these systems according to the particular concept that they support. Access control systems provide protection by establishing a checkpoint at entry points to a building through which only authorized persons may pass. Detection systems look for dangerous objects and agents on persons, their belongings, and their vehicles at a building's entry points. Intrusion detection systems monitor for security incursions throughout a building to alert security staff to react to investigate and contain the intrusion.

Access Control Systems

The first line of security within a federal building is to channel all access through entry control points where identity verification devices can be used for screening. These devices "authenticate" individuals seeking entry, i.e., they verify that the individuals are indeed authorized by electronically examining credentials or proofs of identity.

Identity verification devices use three basic technological approaches to security based on something you have, something you know, and something you are. Accordingly, they range from automatic readers of special identification cards (something you have), to keypad entry devices that generally require a pin number or password (something you know), to more sophisticated systems that use biometrics (something you are) to verify the identity of persons seeking to enter a facility. More secure access control systems use a combination of several of these approaches at the same time for additional security.

Technologies used by identity verification devices include the basic bar code or magnetic strip for card-swipe readers, similar to those used for credit cards, cards that use radio frequency signals and need only be

passed within close proximity to a reader to identify the card holder, and smart cards that can contain biometric identifiers. Keypad entry devices are often used in combination with cards and card readers. Newer access control systems that use biometric technologies to verify the identity of individuals can significantly increase building security.

The term biometrics covers a wide range of technologies used to verify identity by measuring and analyzing human characteristics. Identifiable physiological characteristics include fingerprints, retinas and irises, and hand and facial geometry. Identifiable behavioral characteristics are speech and signature. Biometrics theoretically represent a very effective security approach because biometric characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed.

Biometric systems first capture samples of an individual's unique characteristic that are then averaged to create a digital representation of the characteristic, known as a template. This template is stored and used to determine if the characteristic of the individual captured by the identity verification device at the entry control point matches the stored template of that individual's characteristic. Templates can be stored within the device itself, in a centralized database, or on an access card.

Until recently, in addition to being very expensive, the performance of most biometric technologies had unreliable accuracy. However, prices have significantly decreased and, after years of research, the technology has recently improved considerably. Today biometric devices that read fingerprints and hand geometry have been operationally deployed and proven to be affordable and reliable. Nevertheless, other biometric technologies are not as mature and still tend to falsely reject authorized persons or falsely accept unauthorized persons. These reliability weaknesses will have to be overcome before their use can be widespread. User acceptance is also an issue with biometric technologies in that some individuals find them difficult, if not impossible, to use. Still other individuals resist biometrics in general because they perceive them as intrusive and infringing on their right to privacy.

Once a person is authenticated, access control systems are designed to electronically allow passage through some barrier. Building access barriers can range from such conspicuous physical structures as revolving doors to all but transparent optical turnstiles that generate an alarm when an unauthorized individual attempts to pass.

Table 1 provides a high-level description of access control technologies that can be deployed to protect federal facilities. Attachment I describes the technologies in greater detail.

Table 1: Access Control Technologies

Technology	How the technology works	Effectiveness	Performance factors	User acceptance
Biometrics				
Fingerprint scan	Patterns of fingertips are captured and compared	Reliable	Dirty, dry, worn fingertips	Medium, some resistance based on association with law enforcement
Hand geometry	Dimensions of hand and fingers are measured and compared	Fewer unique characteristics measured	Injuries and jewelry	Good, but may require minimal training
Retina scan	Patterns of blood vessels on retina are captured and compared	One of most accurate biometrics	Hardest to use of biometric technologies	Considered intrusive
Iris scan	Patterns of iris are captured and compared	One of most accurate biometrics	Lighting and movement	Medium, some resistance based on sensitivity of eye
Facial recognition	Facial features are captured and compared	Dependent on lighting, positioning, updating reference template	Environmental factors	Good, but some concern about possible misuse
Speaker recognition	Cadence, pitch, and tone of vocal tract are captured and compared	Better suited for other applications	Environment, inconsistencies, and quality of equipment	Good
Signature recognition	Rhythm, acceleration, and pressure flow of signature are captured and compared	Better suited for other applications	Erratic signatures	Good
Access cards				
Magnetic swipe cards	Identification is encoded in magnetic strip on plastic card	Substantially more secure if used in conjunction with other controls	Subject to demagnetization and wear and tear	Good

Technology	How the technology works	Effectiveness	Performance factors	User acceptance
Proximity cards	Identification is encoded in card transmitted by radio frequency antenna	Substantially more secure if used in conjunction with other controls	More durable than swipe cards	Good
Smart cards	Identification data are stored in memory chip	Substantially more secure if used in conjunction with other controls	Requires proper care	Some concern about security of data stored on card
Keypad entry systems	Require users to enter passcodes	Substantially more secure if used in conjunction with access card system	Users may forget passcodes; vulnerable to malfunction and vandalism	Good
Access barriers (turnstiles/revolving doors)	Used in conjunction with access card systems to bar unauthorized access	Only allows authorized access	High traffic flow	Good

Detection Systems

Detection systems provide a second layer of security. Portal (walk-through) metal detectors can be strategically deployed at entry control points to screen individuals for hidden firearms and other potentially injurious objects, such as knives and explosive devices, as they clear the access control system. Unlike more traditional detectors which simply generated an alarm when a metal target was detected anywhere on an individual's body, more technologically advanced portal scanners now come equipped with light bars to highlight the locations where highest metal concentrations are detected. More sensitive and ergonomic handheld detector wands are also now commercially available to perform thorough and rapid follow-up screens.

As individuals proceed through the metal detector, their carried items can be passed through an x-ray system, which scans the items to obtain an image of the contents. Low-energy x-ray systems are also currently being tested to screen individuals for hidden weapons and explosives. However, performance, privacy, and health issues associated with this technology will have to be overcome before it can be widely deployed. Though not yet commercially available, holographic scanning, which can screen for metallic as well as nonmetallic weapons concealed under clothing, is

another new technology currently being tested by the Federal Aviation Administration.

Explosive trace detectors provide an additional layer of building security. Security personnel swab the surface of a person's belongings at entry control points to check for concealed explosives. The swab is then placed into the detection device, which tests for the presence of explosive traces. Portal explosive detection systems and systems that detect large vehicles carrying bombs are now commercially available, but the technology has not yet been widely deployed. Finally, more research and development efforts will be required before technologies for detecting chemical/biological agents become more effective and affordable.

Table 2 provides a high-level description of detection technologies that can be deployed to protect federal facilities. Attachment II describes the detection technologies in greater detail.

Table 2: Detection Technologies

Technology	How the technology works	Effectiveness	Performance factors	User acceptance
X-ray scanning systems	Electromagnetic waves (x-rays) are used to allow distinct structures to be viewed on a monitor. Due to differences in material compositions, items are distinguishable.	Persons familiar with the exact construction of a particular x-ray system could pack a bag to make a threat item difficult to recognize.	Depend on the efficiency of the operator and the amount of clutter in a bag or on a person.	Some concern about exposure to radiation.
Metal detectors	Used to locate concealed metallic weapons on persons. When the detector senses a questionable item or material, an alarm signal is produced	Considered a mature technology. Can accurately detect the presence of most types of firearms and knives. However, they are typically not accurate when used on objects that contain a large number of different materials.	Can be extremely sensitive to interference from conflicting signals of nearby objects. Traffic flow depends on well-trained and motivated operators. Portal detectors require frequent adjustment.	Some concern about exposure to the magnetic field of metal detectors. Issues of privacy and discrimination have also been raised.
Explosive detection systems	Used to detect bulk or trace explosives concealed in, on, or under vehicles, containers, packages, and persons.	Technology capable of detecting most military and commercially available explosives. However, most systems designed to detect only a subset.	Depend on the method used to collect sample and operator efficiency.	Explosive detection units are not intrusive.

Intrusion Detection Systems

Intrusion detection systems alert security staff to react to potential security incidents. CCTV cameras play an integral part of intrusion detection systems. Security personnel can use this technology to monitor activity throughout a building, in particular at entryways, exits, stairwells, and other areas that are susceptible to intrusion. CCTV technology is

mature, practical, and reasonably priced. Moreover, it is highly cost efficient because one person can monitor several areas on different screens at the same time from one central location. However, experiments have shown that relying on security staff to detect incidents by constantly monitoring scenes from the camera in real time is ineffective. Because watching camera screens is both boring and mesmerizing, the attention of most individuals has degenerated to well below acceptable levels after only 20 minutes of viewing. This is particularly true if staff are watching multiple monitors simultaneously. A more practical application of CCTV is to interface the CCTV system with electronic intrusion detection technologies, which alert security staff to potential incidents requiring monitoring.

Electronic intrusion detectors are designed to identify penetrations into buildings through vulnerable perimeter barriers such as doors, windows, roofs, and walls. These systems use highly sensitive sensors that can detect an unauthorized entry or attempted entry through the phenomena of motion, vibrations, heat, or sound. Examples are technologies that detect motion through breaks in a transmitted infrared light beam and heat emitted from a warm object, such as a human body.

When an intrusion is sensed, a control panel to which the sensors are connected transmits a signal to a central response area, which is continually monitored by security personnel. The sensor-detected incident will alert security personnel of the incident and where it is occurring so that personnel will know what monitor to pay attention to. By interfacing these technologies, security personnel can initially assess sensor-detected security events before determining how to react appropriately. Alarm-triggered video recorders can also be installed to provide immediate playback of a detected event for analysis.

Table 3 provides a high-level description of intrusion detection technologies that can be deployed to secure federal facilities. Attachment III describes the technologies in greater detail.

Table 3: Intrusion Detection Systems

Technology	How the technology works	Effectiveness	Performance factors	User acceptance
CCTV	A visual surveillance technology for monitoring a variety of environments and activities. Typically involves a dedicated communications link between cameras and monitors.	The clarity of the pictures and feed can be excellent. Cameras vary in size, light sensitivity, resolution, type, and power.	Often not effective as an active surveillance tool because of security staff's inattention.	Concern about misuse to track people, racially discriminate, and engage in voyerism.
Intrusion sensors (line sensors, video motion detectors, balanced magnetic switches, and sonic and vibration sensors)	Detect penetrations into secure areas through walls, roofs, doors, and windows. Detection is usually reported by an intrusion sensor and announced by an alarm, which must be followed by a human assessment to determine proper response.	Reliable.	Susceptible to nuisance alarms which can be generated by animals, blowing debris, lightning, water, and nearby traffic. Any disturbance in the electrical power will affect performance.	Users cannot freely open and close windows and doors that have been equipped with sensors.

Technology is Not a Panacea

Although the newer technologies can contribute significantly to enhancing building security, it is important to realize that deploying them will not automatically eliminate all risks. Effective security also entails having a well-trained staff to follow and enforce policies and procedures. Moreover, the technical capabilities of security systems must not be overestimated. Finally, a broad framework of supporting functions must be in place at the federal, state, and local levels.

Technology Cannot Compensate for Human Failure or Ineffective Security Processes

Effective security requires technology and people to work together to implement policies, processes, and procedures that serve as countermeasures to identified risks. To illustrate this point, let us examine the following scenario: an organization has policies in place to mitigate the risk of an outsider committing a harmful act against its employees. One policy states that entry to the building is restricted to authorized personnel and another that no weapons may be brought into the building. An access control system implements the first policy by requiring that people wishing to enter present a smart card with a biometric that matches the stored biometric of the authorized person. A detection system implements the second policy by requiring people to pass through a metal detection portal and their belongings to be scanned by an x-ray machine. These procedures ensure compliance with the policies. However, to be effective, security personnel must enforce the policies by following the prescribed procedures. If security personnel allow exceptions to these procedures, they are failing to enforce compliance with the policies. Just as damaging is the lack of effective security processes. For example, if there are no processes in place to handle the entry of employees who have forgotten

their identity access cards, a vulnerability may be created that could be exploited by adversaries.

Breaches in security resulting from human error are more likely to occur if personnel do not understand the risks and the policies that are put in place to mitigate them. Training is essential to successfully implementing policies by ensuring that personnel exercise good judgment in following security procedures. In addition, having the best available security technology cannot ensure protection if people have not been trained in how to use it properly. Training is particularly essential if the technology requires personnel to master certain knowledge and skills to operate it. For example, x-ray inspection systems rely heavily on the operator to detect concealed objects in the generated x-ray images. If security personnel have not received adequate training in understanding how the technology works and detecting threat images, such as a knife, the security system will be much less effective.

The Capabilities of Security Technologies Can Be Overestimated

It is also important to determine how effective technologies really are. Are they actually as accurate as vendors state? In overestimating their capabilities, security officials risk falling into a false sense of security and relaxing their vigilance.

During our review, we found instances in which the performance estimates vendors provided for some of their biometric technologies were far more impressive than those obtained through independent testing. As always, it is important to keep in mind the adage of "buyer beware" when making procurement decisions. There are publicly available resources that provide assessment guidance regarding security products. For example, the National Institute of Justice has evaluated a number of security products over the past few years and can serve as a valuable resource to federal agencies for making purchasing decisions.[8]

Also bear in mind that lesser technological solutions sometimes may be more effective and less costly than more advanced technologies. Dogs, for example, are an effective and time-proven tool for detecting concealed explosives. The dogs currently used by DoD, for example, can detect nine different types of explosive materials. And since dogs have the advantage of being mobile and able to follow a scent to its source, they have significant advantages over mechanical explosive detection systems in any application that involves a search.

[8]See http://www.ojp.usdoj.gov/nij/about_sci.htm.

The Involvement of Multiple Government Entities is Required to Secure Federal Facilities

The use of technologies as countermeasures is identified in the final step of the risk management process. As such, they are only capable of defending against recognized threats. If unrecognized threats are not factored into the risk management process, these risks will not be mitigated and the technologies that have been implemented may be ineffectual in preparing for them.

Security managers of federal buildings rely on federal, state, and local government entities to prevent, detect, and respond to acts of terrorism against their facilities. Federal security managers typically are not aware of potential threats posed by foreign and domestic terrorist groups. As such, they depend on intelligence and law enforcement agencies such as the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research to gather information about and assess such threats against their facility.

Security managers of federal buildings also do not have access to the range of emergency resources required to respond to terrorist attacks. They rely on state and local governments to provide fire-fighting, medical personnel, and other emergency services. They also rely on the police and the judicial systems to enforce and prosecute violators of the laws and regulations governing the protection of federal buildings.

Substantial Challenges Remain

Despite significant advances in performance and capability, the newer security technologies still face considerable technical challenges and user acceptance issues before they can be effectively integrated and widely deployed in federal facilities.

The Lack of Standards Impedes System Integration

First, because there are no industrywide common standards for data exchange and application programming interfaces[9] for technologies that provide physical security, most of the equipment used by the technologies in our review is not interoperable. For example, deploying an access control system that uses a smart card containing a fingerprint biometric would require at least three pieces of equipment: the card reader device, the fingerprint scan device, and the hardware device used to house and operate the biometric software. If these devices are made by different manufacturers, they cannot function as an integrated environment without software to connect the disparate components. Not only does developing the initial customized software represent substantial expenditures, but

[9]The interface between the application software and the application platform (i.e., operating system), across which all services are provided.

new software will have to be developed whenever old equipment is replaced by equipment from a different manufacturer. Moreover, standardizing on one manufacturer's equipment is not the most advantageous option since doing so leaves no range of equipment from which to choose and requires replacing all existing hardware not made by that manufacturer. Although efforts are underway to address the lack of standards, it will be some time before this problem is resolved.

The Use of Several Security Technologies Continues to Generate Concerns about their Potential Violation of Expectations of Privacy

Second, Americans expect and cherish the value and freedom of privacy. Recent concern within Congress and public interest groups alike about the intended use of CCTV by D.C. law enforcement agencies has highlighted issues regarding the consequences of the applications of newer security technologies on privacy.[10] In general, apprehensions are based on a fear of misuse, i.e., that these security technologies will be used for purposes other than for which they were intended. For example, there is a fear that the government may use the newer surveillance technologies to track people. In addition, employees fear that management will be tempted to monitor their performance. Also at issue is whether people will be arbitrarily monitored based on their race or ethnic origin or whether operators may be tempted to indulge in video voyeurism by, for example, especially focusing on young, attractive females.

Another concern is that biometric technologies may reveal confidential medical information. Because diseases such as AIDS, diabetes, and high blood pressure cause changes to the retina, some people fear that retinal scans could compromise the privacy of this information.

Civil liberties advocates also find the newer detection system technologies too intrusive. The tremendous potential for embarrassment was recently pointed out by newspapers reporting on low-dose x-ray systems installed at Orlando International Airport that essentially perform "virtual strip searches." These systems, now in a test phase, can see a person's body through clothing. Newspapers published pictures revealing images of a person's body—every inch of it—graphically captured by the scanner.

Not All Security Technologies Are User Friendly

Third, several of the security technologies we reviewed have the disadvantage of being both complex and inconvenient to use, requiring considerable user cooperation. Most biometric technologies, in particular, have some negative features. Retina scanning, for example, feels

[10]The House Committee on Government Reform, Subcommittee on the District of Columbia held a hearing on the expanding use of electronic surveillance in the District of Columbia on March 22, 2002. During the hearing, the chairwoman and ranking minority member of the subcommittee emphasized the need for policies, procedures, and guidance to govern the use of CCTV technology because of the potential infringement on the public's privacy rights.

physically intrusive to some users because it requires close proximity with the retinal reading device. Moreover, fingerprinting feels socially intrusive to some users because of its association with the processing of criminals.

There is also an assortment of health concerns among a segment of the population regarding certain security technologies. There is evidence that pacemakers and hearing aids can be adversely affected by some detection technologies. However, no evidence has been produced to substantiate fears of radiation exposure from x-ray systems and apprehensions that certain detection systems could cause depression or even brain tumors. Certain groups of individuals resist using biometric devices because of hygiene issues.

In conclusion, our review has identified myriad commercially available technologies that implement the three essential concepts of effective security: protection, detection, and reaction. Many of these technologies are mature and have already been deployed in various federal facilities, where their capabilities and effectiveness have been demonstrated. Other newer technologies appear to offer great potential in helping federal agencies to ensure the security of their facilities. These technologies could be adopted in the near future. Other technologies are still in a nascent stage of development, but are maturing and appear promising. Many biometric technologies still face barriers in intrusiveness and complexity that must be addressed before they can be most effectively deployed and widely accepted by users. However, they offer greater security, and the challenges to their implementation may not be formidable.

However, of foremost importance is to continue to bear in mind that effective security can never be achieved by relying on technology alone. People will always play a fundamental role in all phases: from planning to implementation and to enforcement. Accordingly, technology and people must work together as part of an overall security process, beginning with a risk management approach and incorporating, implementing, and reinforcing those three essential concepts.

Mr. Chairman and members of the subcommittee, this concludes my statement. I would be pleased to answer any questions you or the members of the subcommittee may have.

Contacts and Acknowledgment

For further information, please contact me at (202) 512-6412 or via e-mail at rhodesk@gao.gov. Individuals making key contributions to this testimony included Sophia Harrison, Ashfaq Huda, Richard Hung, Elizabeth Johnston, and Tracy Pierson.

(310150)

Attachment I: Access Control Technologies

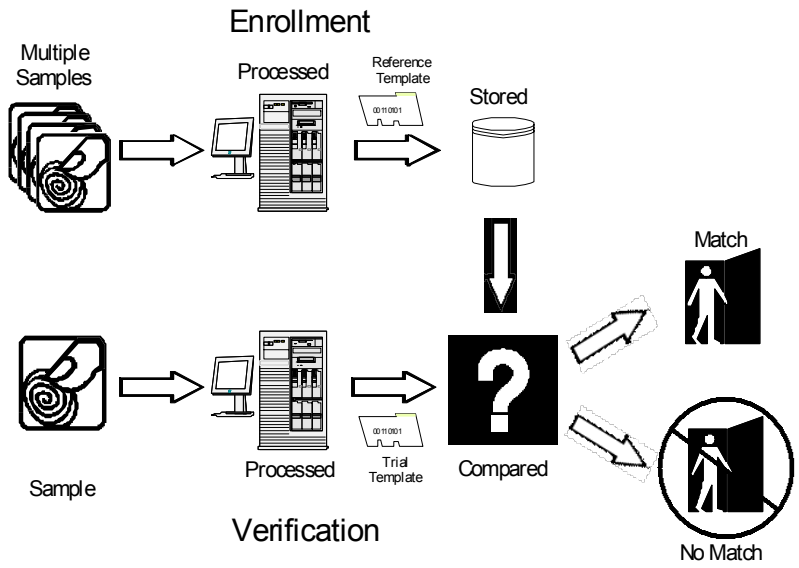
The first line of security within a federal building is to channel all access through entry control points where identity verification devices can be used for screening. These devices "authenticate" individuals seeking entry, i.e., they verify that the individuals are indeed authorized to be there by electronically examining credentials or proofs of identity.

Identity verification devices use three basic technological approaches to security based on something you have, something you know, and something you are. Accordingly, they range from automatic readers of special identification cards (something you have), to keypad entry devices that generally require a pin number or password (something you know), to more sophisticated systems that use biometrics (something you are) to verify the identity of persons seeking to enter a facility. More secure access control systems use a combination of several of these approaches at the same time for additional security.

Biometric Access Controls

The term "biometrics" covers a wide range of technologies used to measure and analyze human characteristics to verify a person's identity. Identifiable physiological characteristics include fingerprints, eye retinas and irises, and hand and facial geometry. Identifiable behavioral characteristics are speech and signature. Biometrics represents a theoretically very effective security approach because these characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed.

Figure 2: Biometric Identification Verification Process



Source: GAO.

Although biometric technologies measure different characteristics, all biometric access control technologies involve a similar process that includes the following components:

Enrollment: multiple samples of an individual's biometric are captured (as an image or a recording) via an acquisition device (e.g., a scanner or a camera).

Reference template: the captured samples are averaged and processed to generate a unique digital representation of the characteristic, which is stored for future comparisons. Templates are essentially binary number sequences. The size of the template depends on the technology, but generally ranges from 10 bytes to 20,000 bytes. It is impossible to recreate the sample, such as a fingerprint, from the template. Templates can be stored centrally on a computer database, within the device itself, or on a smart card.

Verification: a sample of the biometric of the person seeking access to a building is captured at the entry control point, processed into a trial template, and compared with the stored reference template to determine if

they match.[11] Because the reference template is generated from multiple samples at enrollment, the match is never perfect. Therefore, systems are configured to verify the identity of users if the match exceeds an acceptable threshold.

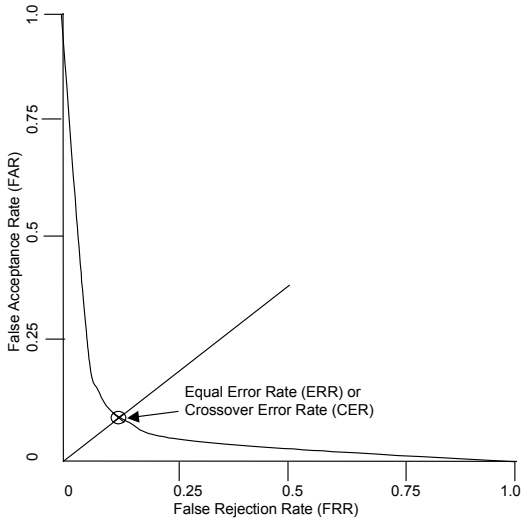
The effectiveness of biometric systems is characterized by two error statistics: false rejection rates (FRRs) and false acceptance rates (FARs). For each FRR there is a corresponding FAR. A false reject occurs when a system rejects a valid identity; a false accept occurs when a system incorrectly accepts an identity. If biometric systems were perfect, both error rates would be zero. However, all biometric technologies suffer FRRs and FARs that vary according to the individual technology and its stage of development.

Because biometric access control systems are not capable of verifying identities with 100 percent accuracy, trade-offs must be considered during the final step of the risk management process when deciding on the appropriate level of security to establish. These trade-offs have to balance acceptable risk levels with the disadvantages of user inconvenience. For example, perfect security would require denying access to everyone. Conversely, granting access to everyone would result in denying access to no one. Obviously neither of these extremes is reasonable, and access control systems must operate somewhere between the two. How much risk one is willing to accommodate is the overriding factor in adjusting the threshold, which translates into determining the acceptable FAR. The tighter the security required, the lower the tolerable FAR.

Vendors of biometric systems are currently claiming that false accepts occur once out of every 100,000 attempted entries and that the FRR is about 2 to 3 percent. However, because system thresholds are adjusted to accommodate different FARs, it is often difficult to measure and compare their effectiveness. Vendors also describe the accuracy of their systems in terms of an equal error rate, also referred to as the crossover accuracy rate, or the point where the FAR equals the FRR.

[11]Unlike other access control systems, some biometric systems can also identify an authorized user without the user having to present any other identifier, such as an identity card or a pin number or password, by looking through an entire database of authorized users to attempt to find a match. Whereas verification systems attempt to perform one-to -one matches, identification systems attempt to perform one-to-many matches. Systems operating in this mode naturally take longer; the bigger the database, the slower the search. They are also less accurate.

Figure 3: General Relationship between FAR and FRR



Source: GAO.

As shown, selecting a lower FAR increases the FRR—the chance that an authorized person will be denied access to a facility. Perfect security would require denying access to everyone. In this extreme case, the FAR would be "0" and the FRR "1." Conversely, granting access to everyone would result in a FRR of "0" and a FAR of "1."

Attachment I—Access Control Technologies: Biometrics

Fingerprint Scan

Fingerprint scan device.

Source: U.S. Access Board.

Fingerprint scan used for physical access control.

Source: National Coordination Office for Information Research and Development.

How the technology works

Fingerprint scan technology (also known as fingerprint recognition) uses the impressions made by the unique, minute, ridge formations or patterns found on the fingertips. Although fingerprint patterns may be similar, no two fingerprints have ever been found to contain identical individual ridge characteristics. These characteristics develop on normal hands and feet some months before birth and remain constant, except for accidental damage or until decomposition after death.

The image of the fingerprint is captured either optically or electrically.[1] A template is then created from the image. There are two primary methods for creating templates. Most fingerprint scan technologies base the template on minutiae, or the breaks in the ridges of the finger (such as ridge endings or points where a single ridge divides into two). The second method is based on pattern matching of the ridge patterns. In neither method is the template a full fingerprint image, and a real fingerprint cannot be recovered from the digitized template. The generated template ranges from 250 bytes for minutiae-based templates to about 1000 bytes for ridge-pattern-based templates.

Effectiveness

Vendors commonly claim an FRR of 0.01 percent. Despite a low FAR, independent testing has shown that some scanning devices can have a FRR of nearly 50 percent.

[1]A third method, using ultrasound technology, is not yet widely used.

Performance factors	In a small percentage of the population, fingerprints cannot be captured because a person's fingerprints are dirty or have become dry or worn due to age, extensive manual labor, or exposure to corrosive chemicals. In addition, the optical method of fingerprint scanning can be prone to errors if there is a buildup of dirt, grime, or oil on the surface of the device where the image is captured.
User acceptance	Because fingerprints have historically been used by law enforcement agencies to identify criminals, there is some user resistance to this technology. Also, people may have hygienic issues with having to touch the plate of the scanner that has previously been touched by many people.
Vendors	According to a 2001 report published by Gartner Group, Inc., the leading vendors are American Biometric Company, Digital Persona Inc., Identix Inc., and Bioscrypt, Inc. (formerly Mytec Technologies Inc.).
Unit price range	The GSA schedule lists fingerprint readers designed for physical access control at prices ranging from about $1,000 to about $3,000 per unit. Software licenses for the fingerprint technology are listed for about $4.00 per user enrolled.

Attachment I—Access Control Technologies: Biometrics

Hand Geometry

Access control terminal.

Source: Recognition Systems, Inc.

How the technology works

Hand (or finger) geometry[1] is based on the premise that each individual's hands, although changing over time, remain characteristically the same. The technology collects over 90 automated measurements of many dimensions of the hand and fingers, using such metrics as the height of the fingers, distance between joints, and shape of the knuckles. The user's hand is placed on the sensor's surface, typically guided into proper position by pegs between the fingers. Only the spatial geometry is examined; prints of the palm or fingers are not taken. About a 10- to 20-byte template is created from hand geometry.

Effectiveness

Independent testing of the leading hand geometry readers (manufactured by Recognition Systems, Inc.) at Sandia National Laboratories in 1991 produced a FAR of less than 0.1 percent and an FRR of less than 0.1 percent.

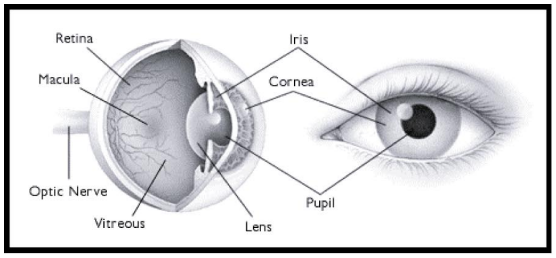
Hand geometry is not considered as robust as other biometric access control technologies because of similarities between individual hand templates. Not as much distinguishing information can be found in a hand compared to an iris or a fingerprint.

[1] Hand geometry uses the entire hand; finger geometry typically uses two or three fingers. However, the technology is the same for both and will be referred to as "hand geometry" in this document.

Performance factors	Hand geometry is a well-developed technology, which disregards fingernails and surface details such as fingerprints, lines, scars, and dirt. However, hand injuries and jewelry can impede accurate readings and/or comparisons. Whether used for verification or identification purposes, the stored image templates must be kept updated as appearances are naturally altered by age.
User acceptance	Hand geometry is considered to be easy to use, although a minimal amount of training is required for users to align their hands in the reader.
Vendors	The hand geometry market is dominated by Recognition Systems, Inc. The finger geometry market is led by BioMet Partners.
Unit price range	Hand geometry reader devices generally cost between $2,000 to $4,000.

Attachment I—Access Control Technologies: Biometrics

Retina Scan



Blood vessels used for biometric identification are located along the retina.

Source: American Academy of Opthamology.

Retina scan device.

Source: EyeDentify Europe N.V.

How the technology works

Retina scan technology is based on the patterns of blood vessels on the retina, a thin nerve about 1/50th of an inch thick located on the back of the eye. These patterns are unique from person to person. No two retinas are alike, not even in identical twins. Retinal patterns remain constant throughout a person's lifetime except in cases of certain diseases.

Retina scan devices project a low-intensity infrared light through the pupil and onto the retina. The patterns of the retina's blood vessels are measured at over 400 points to generate a 96-byte template.

Effectiveness

Retinal scanning, along with iris scanning technology, is the most accurate and reliable of the biometric technologies. It is virtually impossible to replicate the image produced by a human retina. It has been used as a mainstay technology for controlling access to highly secure government facilities.

Depending upon system threshold settings, FRRs can be as low as 0.1 percent and FARs as low as 0.0001 percent (1 in 1,000,000).

Performance factors

Retina scan biometrics are the hardest to use. The older technology requires users to repeatedly focus on a rotating green light through a small opening in the scanning device, located within 1/2 inch of his or her eye, and to hold very still for 10 to 12 seconds at a time. However, a newly developed technology is capable of capturing a retinal image at distances as great as a meter from the user's eye in 1.5 seconds. Also whereas glasses, contact lenses, and existing medical conditions, such as cataracts,

	interfere with the older scanning technology, the newer technology is more accommodating. Though stable over time, the retina can be affected by diseases such as glaucoma, diabetes, high blood pressure, and AIDS.
User acceptance	Even though the technology itself is completely safe, users tend to be resistant to its use because the eye is a very delicate area. Users perceive the technology as intrusive because it requires the use of infrared rays to obtain an accurate reading. Additionally, some users are very hesitant to use the device because the older technology requires close proximity or even contact with the scanner. The newer technology is less intrusive. Some people fear that retinal scans could compromise the privacy of confidential medical information because certain patterns of blood vessels in the retina can be associated with certain diseases.
Vendors	Until recently EyeDentify Inc. was the sole vendor of retina systems. Retinal Technologies, Inc. has lately entered the market with a new retinal scan technology.
Unit price range	Retina scan devices cost approximately $2,000 to $2,500, placing them toward the high end of the physical security spectrum.

Attachment I—Access Control Technologies: Biometrics

Iris Scan

Capturing and verifying user's iris image.

Source: LG Electronics.

How the technology works

Iris scan technology is based on the unique visible characteristics of the eye's iris, the colored ring that surrounds the pupil. The iris of each eye is different; even identical twins have different iris patterns. The iris remains constant over a person's lifetime. Even medical procedures such as refractive surgery, cataract surgery, and cornea transplants do not change the iris's characteristics.

Built from elastic connective tissue, the iris is a very rich source of biometric data. Complex patterns include striations, rings, furrows, a corona, and freckles. Whereas traditional biometrics have only 13 to 60 unique characteristics, an iris has about 266.

A high-resolution black-and-white digital image of the iris is taken to collect data. The system then defines the boundaries of the iris, establishes a coordinate system over the iris, and defines the zones for analysis within the coordinate system. The visible characteristics within the zones are then converted into a 512-byte template.

Effectiveness

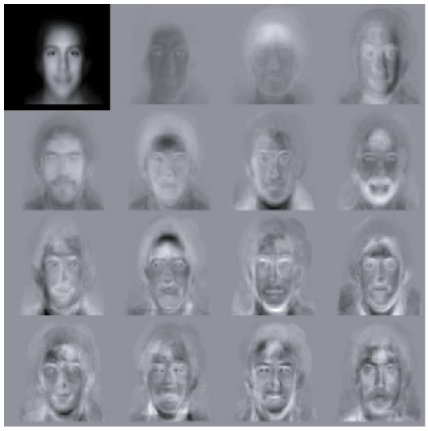
Iris scanning is considered one of the more secure identity verification methods available. Because of the massive quantity of biometric data that can be derived from the iris, the template that is created is unique. In fact, the odds of two different irises returning identical templates is 1 in 10^{52}.

The technology cannot be foiled by wearing contact lenses or presenting an artificial eye to the reading device because algorithms check for the presence of a pattern on the sphere of the eye instead of on an internal plane and use measurements at different wavelengths to detect if the eye is living.

	The Army Research Laboratory recently tested an identification system using iris scan technology from Iridian Technologies. The results indicated an FRR of 6 percent and a FAR of 1 to 2 percent. Few other independent tests of the iris scan technology have been published.
Performance factors	Both the enrollment and verification steps are easy. Contact lenses, even colored ones, normally do not interfere with the process. Wearers of exceptionally strong glasses could have problems, but these could always be removed. Iris recognition can even be used to verify the identity of blind people as long as one of their sightless eyes has an iris. Any unusual lighting situations may affect the ability of the camera to capture the subject. Also, glare and reflections, along with user settling and distraction, can cause interferences.
User acceptance	Unlike other biometric identification verification technologies such as fingerprinting or hand geometry, iris scan technology requires no body contact. Although some users resist technologies that scan the eye, the iris scan is more user friendly than the retinal scan because no light source is shown into the subject's eye and close proximity to the scanner is not required. Users can simply glance into a standard video camera from a distance of about 10 inches and have their identity verified in approximately 2 seconds.
Vendors	According to a 2001 report published by Gartner Group, Inc., Iridian Technologies is the sole owner and developer of iris recognition technology. Vendors licensing iris technology include: EyeTicket Corporation, LG Electronics, and Panasonic.
Unit price range	Iris recognition was traditionally among the most expensive biometric technologies costing tens of thousands of dollars. The significant drop in the price of computer hardware and cameras has brought the price down. However, an iris recognition system still costs approximately between $4,000 and $5,000.

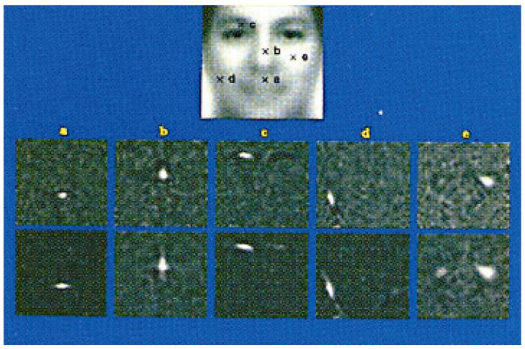
Attachment I—Access Control Technologies: Biometrics

Facial Recognition



Typical Eigenfaces.

Source: MIT Media Laboratory.



Local Feature Analysis.

Source: Visionics Corp.

How the technology works

Facial recognition is a biometric technology that identifies people based on their facial features. Systems using this technology capture facial images from video cameras and generate templates for comparing a live facial scan of an individual to a stored template.

These comparisons are used in either verifying or identifying an individual. Verification systems (also known as one-to-one matching systems) compare a person's facial scan to a stored template for that person, and can be used for access control. In an identification system (or a one-to-many matching system), a person's facial scan is compared to a database of multiple stored templates. This makes an identification system more suited for use in surveillance in conjunction with CCTV to, for example, spot suspected terrorists whose facial characteristics have already been captured and a template generated and stored in a database.

There are two primary types of facial recognition technology used to create templates:

1. Local feature analysis—Dozens of images from regions of the face are captured, resulting in feature-specific fields such as eyes, nose, mouth, and cheeks. These feature-specific fields are used as blocks of a topographical grid. The types of blocks and their positions are used to identify the face. Small shifts in a feature are anticipated to cause a related shift in an adjacent feature.

2. Eigenface method—Unlike local feature analysis, the eigenface method always looks at the face as a whole. A collection of face images is used to generate a set of two-dimensional, grayscale images to produce the biometric template. When a live image of a person's face is introduced, the system represents the image as a combination of templates. This combination is compared to a set of stored templates in the system's database, and the degree of variance determines whether or not a face is recognized.

Modifications of the algorithms used in local feature analysis and eigenface methods can lead to variances which incorporate the following:

- Neural network mapping—Comparisons of a live facial image to a stored template are based on unique global features rather than individual features. Upon a false match, the comparison algorithm modifies the weight given to certain features (such as shadows).
- Automatic face processing—Facial images are captured and analyzed from the distances and distance ratios between features (such as between the eyes).

Effectiveness

Testing of an identification system was performed using the Face Recognition Technology (FERET) database.[1] According to results of recent testing,[2] the typical recognition performance of frontal images taken on the same day is 95-percent accuracy. For images taken with different cameras and lighting, typical performance drops to 80 percent accuracy. For images taken 1 year later, the typical accuracy is approximately 50 percent.

The Army Research Laboratory recently tested an identification system using facial recognition technology. Despite vendor claims of 75 percent correct identification, the testing showed that only 51 percent were correctly identified. Further, the correct identification was in the system's top 10 possible matches only 81 percent of the time instead of the vendor-claimed 99.3 percent.

[1]The FERET program is sponsored by the U.S. Department of Defense Counterdrug Technology Development Program.

[2]In September 1996, the FERET program administered the third in a series of FERET face-recognition tests. These tests used a single gallery containing 1,196 frontal images gathered between 1993 and 1996.

	Facial recognition technology cannot effectively distinguish between identical twins.
Performance factors	The effectiveness of facial recognition technology is heavily influenced by environmental factors, especially lighting conditions. Variations in camera performance, facial position, facial expression, and facial features (e.g., hairstyle, eyeglasses, and beards) further affect performance. As a result, current facial recognition technology is most effective when used in consistent lighting conditions with cooperative subjects in a mug-shot-like position (where hats and sunglasses are removed and individuals look directly at the camera one at a time). Whether used for verification or identification purposes, the stored image templates must be kept updated since appearances are naturally altered by age.
User acceptance	When used in a verification system for access control, facial recognition is typically considered by users to be less intrusive than other biometric technologies, such as iris scanners and fingerprint readers. However, when used in an identification system, there are concerns that this technology can be used to facilitate the tracking of individuals without their consent.
Vendors	According to a 2001 report published by Gartner Group, Inc. the leading vendors are eTrue Inc., Viisage Technology Inc., and Visionics.
Unit price range	For an installation with up to 30,000 persons, a facial-recognition server costs about $15,000. Depending on the number of entry points using facial-recognition technology, software licenses range from about $650 to $4,500.

Attachment I—Access Control Technologies: Biometrics

Speaker Verification

How the technology works

Speaker verification works by creating a voice template based on the unique characteristics of an individual's vocal tract, which results in differences in the cadence, pitch, and tone of an individual's voice.

During enrollment, samples of a person's speech are captured by having the person speak some predetermined information into a microphone or a telephone handset (e.g., name, birth month, birth city, favorite color, or mother's first name). A template is then generated from these "passphrases" and stored for future comparison. When attempting to gain access, the person is asked by the system to speak one or more of the randomly selected enrolled passphrases for comparison.

Some speaker recognition systems do not rely on a fixed set of enrolled passphrases to verify a speaker's identity. Instead these systems are trained to recognize similarities in the voice patterns of individuals when they speak unfamiliar phrases with the voice patterns they are familiar with based on previously enrolled phrases. This is similar to the way in which the human brain instinctively attempts to match an unfamiliar word that it hears with one that it already knows.

The typical biometric voice template is between 10,000 and 20,000 bytes.

Effectiveness

Although speaker verification can be used for physical access control, it is more often used in environments in which voice is the only available biometric identifier, such as telephony and call centers.

Equal error rates for systems that use a fixed set of enrolled passphrases range between 1 and 6 percent, depending on the number of words in the passphrase.

Systems that do not rely on a fixed set of enrolled paraphrases are not as accurate. The more unfamiliar phrases the system is required to compare, the more likely that a false accept will occur.

Performance increases with higher-quality input devices.

Some speaker verification systems provide safeguards against the use of a recorded voice to spoof the system. For these systems, the electronic properties of a recording device, particularly the playback speaker, will

change the acoustics to such a degree that the recorded voice sample will not match a stored voiceprint of a "live" voice.

Performance factors

The enrollment procedure takes less than 30 seconds. The user must be positioned near the acquisition device. Users must speak clearly and in the same manner during enrollment and verification. The typical verification time is 4 to 6 seconds.

Changes in the voice due to factors such as a severe cold might make verifying the voice more difficult. Environmental factors such as background noise also affect system performance. Other factors that can affect performance include different enrollment and verification capture devices, different enrollment and verification environments, speaking softly, poor placement of the capture device, and the quality of the capture device.

User acceptance

Speaker verification systems have a high user acceptance rate because they are perceived as less intrusive than other biometric devices and they are also the easiest to use.

Vendors

According to a 2001 report published by Gartner Group, Inc., the leading vendors are Buytel, T-NETIX Inc., Veritel Corporation, and VeriVoice Inc.

Unit price range

The list price for a 16-door system is $21,000.

Overall speaker verification can cost between $70 and $250 per user.

Attachment I—Access Control Technologies: Biometrics

Signature Recognition

Signature recognition technology used to secure access to a handheld PC.

Source: Bio4.

Signature recognition system using a write pad.

Source: Hesy.

How the technology works

Signature recognition authenticates the identity of individuals by measuring their handwritten signatures. The signature is treated as a series of movements that contain unique biometric data, such as personal rhythm, acceleration, and pressure flow. Unlike electronic signature capture, which treats the signature as a graphic image, signature recognition technology measures how the signature is signed.

In a signature recognition system, the user signs his or her signature on a digitized graphics tablet or personal digital assistant. The system analyzes signature dynamics such as speed, relative speed, stroke order, stroke count, and pressure. The system compares not merely what the signature looks like, but also how it is signed. The technology can also track each person's natural signature fluctuations over time.

The signature dynamics information is encrypted and compressed and can then be stored in a database system, smart card, or token device. The stored template size is 1,500 bytes.

Effectiveness

The use of signature recognition for access control seems fairly limited. A proficient "forger" is quite capable of selectively provoking false accept identifications for individual users.

Performance factors

The typical verification time is from 4 to 6 seconds.

Several performance factors may impede signature verification. These include a user signing too quickly, a user having an erratic signature, a signature that is particularly susceptible to emotional and health changes, and using different signing positions.

	Enrollment usually requires several consistent captures.
User acceptance	The system is easy to use, non-intrusive, and requires no staff or customer training, nor any alteration in signing modes or habits. Because dynamic signature verification closely resembles the traditional signature process, it has minimal user acceptance issues. The graphics tablet can be inconvenient as an input device. While the principal criticism is that the person does not see what he is writing, the rather soft base on which the person signs also takes some getting used to.
Vendors	According to a 2001 report published by Gartner Group, Inc., the leading vendors are Communication Intelligence Corporation and Cyber-SIGN Inc. Additional vendors include Hesy, WonderNet, and ScanSoft.
Unit price range	A signature recognition tablet costs about $375.

Attachment I—Access Control Technologies: Access Cards

Magnetic Swipe Cards

Magnetic swipe card.

Source: HID Corp.

Magnetic swipe card reader.

Source: IDenticard.

How the technology works

Systems based on magnetic swipe cards allow users to access buildings by inserting or swiping a uniquely coded access card through a reader. Magnetic swipe cards have a narrow strip (magstripe) of magnetic material fused to the back of a plastic card, which is very similar to a piece of cassette tape. The size of the card and the position of the magnetic strip are set by the International Organization for Standardization (ISO) standards. A typical bank or credit card is an example of a magnetic swipe card.

The principle of an access control system that uses magnetic swipe technology is that a unique number is encoded onto the user card. The card reader reads the number that the access control unit interprets and in conjunction with a database determines if the user is authorized.

Most magnetic swipe card readers use one of two methods for reading the card:

- Swipe reader—A card is swiped through a long, narrow slot that is open at each end.
- Insert reader—A card is inserted into a small receptacle that is just large enough to accommodate the card.

The security swipe card may be for general access, meaning that the card does not provide data about the person using it, or it may be individually encoded, containing specific information about the cardholder. Typically, the data on an encoded security swipe card can include:

- name
- ID number (social security number or other unique number), and

	• access level when different offices within a facility require different levels of access.
Effectiveness	Magnetic swipe card systems perform effectively. However, a magnetic swipe card system still does not necessarily verify a person; it only confirms that the person has a card. For this reason, these systems are generally not considered acceptable as stand-alone systems for high security areas and require additional controls, such as PINs or biometric identification. Coded credentials are also vulnerable to counterfeiting and decoding. A card that is lost or stolen can be used by unauthorized persons. Additionally, if the authorized access lists are not frequently updated, the potential exists for persons who no longer have authorization to gain access to a secure area. As a result, a magnetic swipe card system is considered more effective when combined with other methods of authentication, such as a keypad entry system or biometrics.
Performance factors	The most common problem with the magnetic swipe card is the inability to be read by the card reader. Because they have to be durable enough to withstand repeated use, magnetic swipe cards are wrapped in a single piece of protective laminate that protects them from demagnitization, a common cause of card failure in reader systems. The wrapper also protects them from cracking or chipping. Even then, wear and tear will affect the card itself; dirty or scratched cards are also unreadable. The Defense Protective Service has complained that the problem with its current access control magnetic swipe cards is that the magnetic strip wears down within a year of use.
User acceptance	Overall there are no user acceptance issues with the magnetic swipe card.
Vendors	According to the Security Industry Association, the leading vendors are Mercury, Apollo, and Doavo.
Unit price range	The magnetic swipe cards themselves are very inexpensive at around $1 each. Card readers cost between $150 and $300 each.

Attachment I—Access Control Technologies: Access Cards

Proximity Cards

Proximity card and card reader.
Source: HID Corp.

How the technology works

Proximity cards are passive, read-only devices. They can be of various sizes ranging from a token (about the size of a watch battery) to the size of a credit card.

Proximity cards contain an embedded radio frequency (RF) antenna. The proximity card reader constantly transmits a low-level fixed RF signal that provides energy to the card. When the card is held at a certain distance from the reader, the reader's RF signal is picked up by the card's antenna and absorbed by a small coil inside the card that powers the card's microchip. Once powered, the card transmits to the reader a unique identification code contained in the card's microchip. The whole process is completed in microseconds. Cards can usually be read through a purse or wallet and through most other nonmetallic materials.

The reader can be surface-mounted or concealed inside walls or special enclosures. It can even function behind glass, plaster, cement, or brick, depending on the range. It has no openings that can jam or be tampered with. Card and reader orientation is not critical, and keys or coins held in contact with the card will not alter its code or prevent accurate readings. Reading ranges primarily depend on the reader. The larger the reading range, the larger the size of the reader.

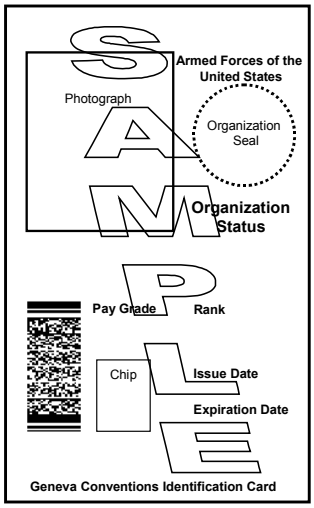
Effectiveness

Proximity card systems perform effectively. However, a proximity card system still does not necessarily verify a person; it only confirms that the person has a card that was issued to the person he or she claims to be. For this reason, these systems are generally not considered acceptable as stand-alone systems for high-security areas, and require additional

	controls, such as PINs or biometric identification. Additionally, authorized access lists must be frequently updated to ensure that access authorization remains current. As a result, a proximity card system is considered more effective when combined with other methods of authentication, such as a keypad entry system or biometrics.
Performance factors	The user has to make sure to hold the card facing the reader. The card can typically be verified in less than one second. The contactless nature of the cards reduces the wear and tear associated with cards requiring contact, such as magnetic swipe cards.
User acceptance	Proximity cards are nonintrusive and very easy to use. If a reader has a range of 1 meter, then a proximity card can be worn on a clip or chain and users can gain access by simply passing by the reader.
Vendors	According to the Security Industry Association, the leading vendors are Hughes Identification Devices (HID), Indala, and Applied Wireless Identifications.
Unit price range	Proximity cards cost about $5 to $6; readers can cost up to $750.

Attachment I—Access Control Technologies: Access Cards

Smart Cards



Skeletal image of a smart card.

Source: DoD Defense Manpower Data Center.

How the technology works

Smart cards, about the size and shape of a credit card, are used in access-control systems to verify that the cardholder is the person he or she claims to be. They are increasingly used in one-to-one verification applications that compare a user's biometric (commonly a fingerprint or hand geometry) to the biometric template stored on the smart card.

Smart cards contain a memory chip to store identification data and often have a microprocessor to run and update applications. Most smart cards in use today have the capacity to store 8 kilobytes or 16 kilobytes worth of information, and cards with 32-kilobyte and 64-kilobyte capacities are also becoming available.

There are two types of smart cards: contact cards, which work by being inserted in a smart card reader, and contactless cards, which use radio frequency (RF) signals and need only be passed within close proximity to a card terminal to transmit information. Card readers and terminals are generally very compact and can be mounted on turnstiles and doors.

An advantage of smart cards is that they can support more than one application. For example, they can be used to authenticate physical access to multiple facilities or to specific rooms within a facility, and even to authenticate access to computers or networks.

Effectiveness

Although the smart card industry has made use of experiences from traditional magnetic swipe cards, card reliability is not easy to predict. Physical interfaces for smart cards have been standardized through the ISO,[1] and manufacturers claim that their products pass the ISO reliability tests meant to simulate "real life" conditions. However, each implementation of smart cards varies due to differences in usage patterns, environmental conditions, software, and readers/terminals.

A smart card system still does not necessarily verify a person; it only confirms that the person has a card. For this reason, these systems are generally not considered acceptable as stand-alone systems for high-security areas and require additional controls, such as PINs, or biometric identification. As a result, a smart card system is considered more effective when combined with other methods of authentication, such as a keypad entry system or biometrics.

One government use of smart cards encountered problems because of network performance issues. Specifically, the response time for passing information between the card readers or terminals and the central database was slow, and officials could not readily verify the identification of users trying to access these facilities, causing congestion problems. Further testing revealed that the plastic cards, interfaces or workstation connections, card readers, and terminals worked effectively—though some interface devices worked slower than others.

Performance factors

Consistent performance of smart cards relies heavily on cardholder education about proper card care. Inappropriate user actions (such as punching a hole in the card or using it to scrape ice off a car windshield) are common and should be planned for. Glitches in card reader/terminal software and hardware can also damage smart cards, and it is important to implement mechanisms that identify faulty software and hardware.

User acceptance

Public policy organizations continue to be concerned about the data that will be stored and transferred to databases from smart cards and how government organizations will use the information. As such, some individuals may be reluctant to carry one card for multiple purposes.

[1]ISO standard 7816.

There is no requirement for smart card technologies to meet a minimum set of security standards, and smart cards may be vulnerable to various types of cyber attacks because the devices often support multiple applications that interface with other computerized products. The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are currently working on an evaluation program to certify the security of smart card technologies.

Vendors

The dominant vendors of smart cards are Gemplus and SchlumbergerSema, although many vendors offer security systems based on smart cards. Major smart card system vendors include ActivCard S.A., RSA Security, and Spyrus. At the federal level, the General Services Administration awarded a $1.5 billion contract in 2000 to five vendors—PRC/Litton, EDS, 3-G International, Logicon, and KPMG—to provide federal agencies with a range of smart card services. Under the contract, more than 140 additional vendors have been used to supply federal agencies with software, cards, card readers, terminals, and other peripheral smart card devices—including Nokia, Microsoft, Rainbow Technologies, and others.

Unit price range

The unit price for smart card technology varies and largely depends on the applications and security features supported by the device. The price for the smart card itself can range from about $3 to $30 each. The more applications supported by the smart card, the higher the unit price. Card readers or terminals also range in unit price starting from about $16 per unit. In addition to these costs, organizations incur expenses for managing the associated databases and software as well as issuing the cards to users and administering their use.

Attachment I—Access Control Technologies Keypad Entry Systems

Keypad Entry Systems

Keypad entry system.

Source: GAO.

How the technology works

When used with doors fitted with electric or magnetic locks, keypad entry systems selectively allow users to enter buildings or other secured areas by requiring them to first enter a passcode (a PIN or special code). A standard passcode can be set to allow access to a specific group of individuals, or multiple passcodes can be adopted for each individual to be assigned a unique code. When an authorized passcode is entered using the keypad (which is similar to the numeric keypads of ATM bank machines), the system activates the electric or magnetic lock, unlocking the door for only a brief period of time. A database may be automatically updated each time a passcode is entered to document both successful and unsuccessful access attempts.

Keypad devices typically include a duress function, where a person being threatened can activate a silent alarm to summon assistance. In some systems, the threatened user would enter a specific duress code, whereas in others the threatened users would enter their usual passcode followed by additional digits. In either case, access would be granted in a seemingly normal manner, but a silent duress code would be sent to a designated monitoring station.

A variety of keypads are available, from very simple entry devices to unique keypads that scramble the numbers differently for each use. Although they can be used on their own in an access control system, keypads are typically used in conjunction with an ID card and card reader.

Effectiveness	In a card-reader-only system, an individual must present something they have (an authorized card) to gain entry. However, users of a keypad-only system must only know of an authorized passcode. As such, once a user shares a legitimate passcode, further use cannot be prevented unless the code is changed. Also, as users enter their passcodes, they are susceptible to their codes being "stolen" by a person looking over their shoulder. A keypad entry system is considered more effective when combined with a card system, providing a higher level of security than just the keypad alone.
Performance factors	Keypad entry systems provide a flexible solution for controlling the movement of groups of people or individuals, as the passcodes can be disabled when they are no longer appropriate. However, keypad entry systems, in a manner similar to passwords on computer systems, can be prone to users forgetting their passcodes; hence, requiring other procedures to pass through the door. Keypads are vulnerable to mechanical malfunction as well as vandalism.
User acceptance	User acceptance is high for keypad systems.
Vendors	A selection of vendors taken from the GSA Schedule includes Radionics, Securitron Magnalock Corp., Ideskco Corp., Ultrak, Inc., Vikonics, Inc.
Unit price range	Simple stand-alone keypads, hooked directly to an electric door lock, may cost less than $200 for all the necessary hardware. More sophisticated keypad systems that may be part of a network of keypads can cost from $1200 to several thousand dollars.

Attachment I—Access Control Technology: Access Barriers

Access Barriers

Optical turnstile.

Source: Gunnebo Omega, Inc.

How the technology works

Turnstiles and revolving doors are access barriers that can be installed to continuously control and monitor every individual entering and or exiting a building. Whereas revolving doors are most often deployed to control the entry to a building from the street, turnstiles are usually set within the lobby of a building.

There are a variety of different models of turnstiles that use different technologies. The traditional physical barrier turnstile is the type used in many large business facilities, amusement parks, stadiums, and subway systems. A metal bar is locked into a blocking position to prevent anyone who has not been authorized via some form of identity verification or form of payment, such as a token, from walking through the passageway. When authorization is granted, the bar is released and then relocked until the next person is granted access.

An optical turnstile can enable complete control of access to a facility without using a physical barrier. It uses a smart card, proximity card, or magnetic swipe card system, infrared sensors, and an intelligent control unit to detect and count persons walking through a lane or passageway. Access is granted to only one person per card, thus discouraging tailgating. If a person walks through the passageway without authorization, an alarm is generated.

Optical turnstiles are easy to use and are almost transparent to users. Visual or audio indications are given to the user to indicate various functions such as the open/closed status of the lane, whether the user is authorized to pass through the lane or not, or whether an unauthorized access has been attempted. All activity—including card presentations, reset, unauthorized card presentation, alarms and access attempts—can be monitored and logged by the system controlling the turnstiles. Because these turnstiles function automatically, they only need monitoring by a

Barrier turnstile.

Source: Courtesy of Gunnebo Omega, Inc.

Revolving doors begin to turn as soon as card reader successfully scans an employee's badge.

Source: Horton Automatics.

guard for illegal access attempts or to change lane directions at, for example, different times of the working day.

Like turnstiles, security revolving doors are used to control access to buildings by a card reader verification system, but this technology is usually installed at points of entry from the street. Security revolving doors use either ultrasonic or weight sensors to detect unauthorized access such as piggybacking, where two people try to go through the door at the same time in the same door section, and tailgating, where a person tries to go through the door at the same time as an authorized person in a different section. In the event of an unauthorized access, the door will be reversed so that the unauthorized person remains on the proper side of the door. Security revolving doors can come equipped with voice annunciators that warn unauthorized individuals to exit the revolving door and can cause the door direction to reverse and force the intruder out.

Effectiveness

Turnstiles can detect and accurately report two people walking one behind the other, very close to each other, as long as they are ¼" apart. They can also detect people trying to defeat the turnstile by crawling through or rolling through on a cart. Turnstiles cannot normally detect two people walking side-by-side in lockstep, but turnstile lanes are made narrow enough that this is impractical.

Security revolving doors can increase security by detecting and stopping two or more people trying to pass through the door simultaneously. When the scanning system detects unauthorized passage, the doors come to a controlled stop, and then slowly reverse, thus keeping the violator from passing through. Violations can be logged and reported.

Performance factors

Optical turnstiles can have a traffic flow rate as high as 30 people per minute, or 1800 people per hour, per walkway.

Most revolving door systems are capable of processing almost 1,000 passages per hour in either direction.

Turnstiles with barrier arms are equipped with safety sensors on either side of the barrier arm, so that if someone tries to run through the turnstile as the barriers are closing, the barriers will react quickly and retract.

Revolving doors have a number of built-in safeties that prevent people from being locked in or stuck in the door. They can be operated manually in case of a power failure. When, for whatever reason, one of the doors jams, the other door will turn to an open position. And, they are equipped with an emergency button to stop the door at any desired moment. In addition, the door wings are collapsible, creating a wide and safe escape route in an emergency. Only when the collapsed door wing has been manually returned into the proper position will the door again revolve automatically.

User acceptance

Turnstiles and revolving doors are both very user friendly. They are unobtrusive and aesthetically pleasing and are effective traffic lanes through which employees can pass with safety and security.

Vendors

Turnstile vendors include Smarter Security Systems Inc., Magnetic Autocontrol Corp., Designed Security Inc., and Gunnebo Omega, Inc.

Revolving door vendors include SafeSec Corporation, Horton Automatics, and Boon Edam.

Places where deployed

Turnstiles are widely deployed in the United States. Examples include: the U.S. Postal Service, the World Bank in Washington, DC, and the Pentagon in Arlington, Virginia. The Washington Metropolitan Area Transit Authority also uses barrier turnstiles and a proximity card to give users access to the train platforms.

Minneapolis-based Target Corp. uses turnstiles at its facility along with a card key, which needs to be swiped before allowing entrance to the facility.

Security revolving doors are in use in governmental administrative and national defense buildings, courthouses, institutions, airports, hospitals, banks and many types of buildings in the U.S. and all over the world, including embassy buildings and foreign government buildings.

Unit price range

Optical turnstiles can be purchased for about $43,000 per portal with a card reader. Individual optical-free barrier turnstiles without readers can cost from about $1,000 - $5,000.

Revolving doors can cost anywhere from $20,000 to $30,000.

Attachment II: Detection Technologies

Detection systems provide a second layer of security. X-ray machines, metal detectors, and explosive detectors can be strategically deployed at entry control points to screen individuals and their belongings for hidden firearms, explosives, and other potentially injurious objects as they clear the access control system.

Attachment II—Detection Technologies: X-ray Scanning Systems

X-ray Scanning Systems

X-ray scanning system for baggage.
Source: GAO.

X-ray image of a suitcase containing a handgun.
Source: Copyright Heimann Systems.

How the technology works

X-ray scanners use technology that exposes a person or object to electromagnetic waves (x-rays), allowing distinct structures to be viewed within the person or object. Due to their differing material compositions, items such as metal knives, plastic weapons, and explosive substances will be displayed differently on a monitor. (This is similar to a medical diagnostic x-ray system that differentiates between bone and organs.) Based on the images displayed on the monitor, a human operator can then determine whether an item of interest warrants further investigation.

There are four primary technologies currently used in x-ray scanning systems for weapons and chemical detection:

1. **Transmission**: An x-ray scanner uses only a single x-ray beam, in which the portion of the beam that penetrates the object under investigation is detected and used to produce the x-ray image. Because materials have different densities and compositions, the x-rays allow distinct structures, particularly metal items, to be viewed within an object.

2. **Backscatter**: Objects are detected based on the images produced from reflected x-rays. As a result, plastic weapons, explosives, and drugs appear bright white on a display monitor.

3. **Multi-view (or dual-view)**: The object under investigation is examined by two x-ray beams coming in at different angles.

4. **Computed Tomography (CT):** Known to most people as CAT scanning, this is the same technology used in hospitals to look deep inside the human body. CT has been adapted for security applications and is used in airports to scan checked baggage. Transmission x-ray

images are taken at many different angles through an object and are put together to produce a three-dimensional image of the object. This allows explosives to be specifically identified and discriminated from other similar, yet harmless, materials.

Different x-ray scanning systems have been developed to examine baggage, mail, vehicles, and individuals. Large amounts of mail or cargo can be examined by a fixed system that can scan an entire pallet of cargo for suspicious items. Larger x-ray systems the size of a truck or an entire building allow vehicles to be examined. Body scanning devices detect contraband hidden on a person by utilizing low-power x-rays to see through clothing, penetrating only a few millimeters below the skin.

Effectiveness

The four x-ray technologies have different levels of effectiveness in detecting various items. Persons familiar with the exact construction of a particular x-ray system could pack a bag to make a threat item difficult to recognize. Accordingly, it has been proposed that a combination of technologies working in unison could significantly improve the detection ability of screeners.

Transmission technology reveals fine details, such as bomb components, and exposes situations where an attempt to camouflage or shield an object has been made. Its strength lies in detecting metallic objects such as conventional knives and firearms, but it may be difficult to separate the image of one object from another. Although backscatter technology is not as effective as transmission technology in identifying metals, it is more effective in detecting explosives, composite weapons, and organic materials such as plastics and drugs. A dual-view system provides two different views of each item, allowing an even clearer view of camouflaged or cluttered items. The CT technique provides maximum sensitivity and accuracy for detecting and identifying materials.

Performance factors

Unlike some metal detectors that can be rendered ineffective by demagnetization, x-ray scanners are not sensitive to their surroundings. Virtually no clearance is needed around the equipment except for space for an operator to sit or stand at the controls. However, the size of the actual equipment may be a factor of effective performance (for example, a truck-sized scanner may present a space limitation for an average-sized federal building).

The throughput of x-ray scanning equipment depends on two things: the amount of clutter in a bag or on a person, and the efficiency of the

operator. Clutter occurs where several dark items are grouped together in an x-ray image, so that the actual size and shape of each item cannot be reasonably detected.

The performance of metal detection systems is closely linked with the performance of their operators. Operators assist with the placement of items to be scanned, work the controls, view the monitor, make judgments regarding each scanned item, and perform any needed manual searches. X-ray scanning equipment only provides an operator the tools to examine persons, baggage, or vehicles; it does not identify weapons or explosives for the operator. It is up to the operator to identify the items of interest from the x-ray image. Hence, adequate training of the operators to properly identify weapons and explosives is paramount to the performance of a metal detection system. Initial training is typically provided by the vendor, but the practice and experience of the operator is an important factor.

User Acceptance

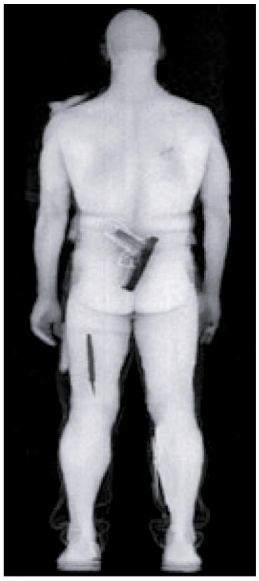
Personal safety issues have been raised, particularly concerns about the exposure to radiation from x-rays. In the unlikely event that a person is exposed to radiation from x-ray equipment used for baggage inspection, studies have shown that this small amount is comparable to that received during an extended air flight. Additionally, research has found that body scanning systems use a very low energy level that is considered safe. Nonetheless, many people find any exposure to x-rays objectionable.

Concerns about the safety of exposing food to x-ray scanners continue to surface, although in 1989 the World Health Organization released a report that supports the safeness of food that has passed through an x-ray device used for cargo. Additionally, with the advancement of x-ray technology to search baggage for explosives, some individuals continue to be wary of allowing camera film to pass through scanners that use higher-power x-rays that could damage film.

New body-scanning equipment used to detect contraband is capable of projecting an image of a passenger's naked body. The use of this equipment may be considered intrusive and raises concerns that a person's privacy would be violated.

X-ray inspection of a truck.

Source: American Science and Engineering Inc.



X-ray image from a body-scanning device.

Source: American Science and Engineering, Inc.

Vendors

Vendors include American Science and Engineering (AS&E), PerkinElmer, Heimann Systems, and Rapiscan.

Unit price range

X-ray scanning devices sized for the detection of materials in baggage range from about $14,000 to $90,000. Equipment used to scan large volumes of cargo can range from around $35,000 to $120,000. Devices for the inspection of trucks and vehicles range from about $1.7 million to $3.7 million. Body scanners cost about $100,000.

Regardless of the function, scanning devices using multiple x-ray technologies (typically a combination of transmission and backscatter) are generally found in the upper end of the price range. Single-technology devices tend to fall in the lower end, with the exception of CT scanning equipment, which costs about $1 million per unit.

Attachment II—Detection Technologies: Metal Detectors

Metal Detectors

Walk through metal detector.
Source: Rapiscan Security Products, Inc.

Handheld metal detector.

Source: Garrett Metal Detectors.

How the technology works

Metal detectors are typically used as a physical security mechanism to locate concealed metallic weapons on a person seeking access to secure areas. When the detector senses a questionable item or material, an alarm signal (either a noise, a light, or both) is produced. Because metal detectors cannot distinguish between, for example, a large metal belt buckle and a metal gun, trained operators are essential to the deployment of metal detectors.

A metal detector senses changes to an electromagnetic field generated by the detector itself. The generated field causes metallic (or other electrically conductive) objects in the proximity to produce their own distinct magnetic fields. The size, shape, electrical conductivity, and magnetic properties of an object are the significant factors used by metal detection technologies to distinguish metal from other detected objects and materials.

Two types of metal detection equipment are commonly used for access control: portal (walk-through) and handheld detectors. Portal detectors are stand-alone structures resembling a deep door frame. Conventional portal detectors alert an operator when metal objects have passed through the portal, but do not indicate the location of the metal objects. However, some of the newer portal systems use a light bar that is located along the side of the portal to pinpoint zones of the body where the metal objects are detected.

After a person who has passed through a portal system has set off an alarm signal, an operator will typically use a handheld metal detector to more accurately locate the object that caused the alarm. These devices are battery-operated and lightweight, allowing the operator to move the wand end of the device around (and within a few inches of) the person's body. When an irregularity in the magnetic field is identified, the handheld device typically emits a loud noise. The operator is then responsible for judging whether the intensity of the signal warrants further investigation.

Effectiveness

Metal detectors are considered a mature technology that can accurately detect the presence of most types of firearms and knives. However, they are typically not accurate when used on objects that contain a large number of different materials (such as purses, briefcases, and suitcases). Government security officials have also reported frequent false alarms and incomplete follow-up scans by security personnel.

Performance factors

Both the portal and handheld metal detectors are designed for use in close proximity situations.

Portal metal detectors are extremely sensitive to interference from conflicting signals of nearby objects. As such, their effectiveness can be easily degraded by a poor location (directly under fluorescent lights or metal air ducts); the nearby use of electromagnetic equipment (such as an elevator); movement from one location to another, and even the placement of a nearby metal trash can. The initial calibrations are generally made by the vendor when the detector is installed. However, facilities often must make adjustments based on results gained through use and their particular security requirements, which determine levels of equipment sensitivities.

Unlike portal metal detectors, handheld metal detectors are not nearly as sensitive to surrounding metal objects. However, the performance of portal metal detectors tends to vary on a daily basis and requires frequent adjustment.

A successful metal detection system depends on well-trained and motivated operators. Typically, an effective operator should be able to process between 15 and 25 people per minute through a portal detector. (This does not include investigation of alarms or other delays.) Traffic flow is generally driven by three factors: the number of devices, the rate at which individuals arrive, and the motivation of individuals to cooperate

with the established procedures. Cooperative individuals can typically be scanned with a handheld detector in about 30 seconds.

User acceptance

Some people, particularly those with certain medical devices such as pacemakers and implantable cardioverter/defibrillators, fear the possible side effects of being subjected to the magnetic field of metal detectors. Because metal detectors emit an extremely weak magnetic field, interactions with walk-through and handheld devices are unlikely to cause clinically significant symptoms. Nevertheless, in 1998 the U.S. Food and Drug Administration began working to address these concerns with both the manufacturers of medical devices and the manufacturers of metal detectors.

Additional issues have been raised regarding the use of handheld metal detectors. Because these devices are passed very closely over the body of individuals who have been selected for further screening, they can be perceived as potential tools for harassment and intimidation. Men wearing turbans and women in undergarments with metal components are examples of two cases that have caused concerns related to discrimination and privacy.

Vendors

There are a number of vendors, including CEIA, Control Screening, LLC, Garrett Metal Detectors, Heimann Systems, Ranger, and Rapiscan.

Unit price range

Portal metal detectors vary widely in price, ranging from about $1,000 to about $30,000. Models in the higher price ranges offer enhanced capabilities, while the lower-range devices may have limited sensitivity and detection capabilities.

Most handheld metal detectors on the market range from about $20 to about $350. As with the portal detectors, capabilities increase along with the price.

Attachment II—Detection Technologies: Explosive Detection Systems

Explosive Detection Systems

A baggage explosive detection unit.

Source: InVision Technologies, Inc.

A portal trace detection device that is capable of detecting and identifying up to 30 different types of explosives, narcotics, and chemical agents.

Source: Barringer.

How the technology works

Several different technologies are currently used to detect explosives: trace detection, quadrupole resonance analysis, and x-ray scanning machines.

The most widely used technology is trace detection, which uses ion mobility spectrometry (IMS) to detect and identify both trace particles and vapors of explosives, narcotics, chemical warfare agents, and toxic industrial chemicals. Trace explosive detection systems can detect a trace of chemicals used in explosives as small as a millionth of a gram. Trace explosive detection equipment comes in a variety of sizes, depending on whether it is to be used to detect chemicals concealed on individuals, in containers, packages, or in or under vehicles.

The handheld explosive detection unit can be used almost anywhere. The device, which is small and lightweight, is capable of detecting over 30 substances in seconds.

Handheld explosive detection unit.
Source: Barringer.

Portable explosive detection unit.
Source: ION Track Instruments.

Tabletop units are becoming common for the detection of explosives concealed in baggage. For these units, which also use IMS technology, security personnel rub the outside of a bag, such as a lock or handle or zipper, with a cotton swab and then insert the swab into a machine that heats the swab, turning the sample into vapors. The unit alerts the operator to the presence of any explosive traces that warrant further examination. Some systems create different sounds to indicate the relative density of the contraband detected and indicate probable drug or gun type materials.

Portal explosive detection units take in the air from around the subject as he or she walks through to check for explosive residue. When explosives are detected, the system sets off a visual and audible alarm, and lists the material identified. It can detect organic and inorganic contraband on the body and clothing.

Quadrupole resonance analysis is another type of technology used to detect explosives. Similar to magnetic resonance imaging (MRI) used in hospitals, this technology is typically used to scan belongings and baggage. These units resemble x-ray machines used for the same purpose.

X-ray machines can also be used to detect explosives and are available to scan belongings, people, or moving and stationary vehicles.

Effectiveness

While the technology is capable of detecting most military and commercially available explosives—including TNT, plastic explosives, high-vapor explosives, and chemical warfare agents—most devices are

designed to detect only a subset. Others have slow processing rates for larger items.

As with other technologies, explosion detection equipment also has a small percentage of false alarms.

Performance factors

All explosive detection systems have specific sampling guidelines for specific applications. This is important because some systems rely almost entirely on the skills of the operators.

Handheld detection devices are lightweight and ready to operate within 1 minute from the time they are turned on. They are easy to use, and provide readings within seconds. The use of these devices near idling cars has been shown to cause interference and require frequent recalibrations.

Tabletop trace detection units are self-calibrating and also provide readings within seconds.

Baggage x-ray machines also provide rapid readings and can process an average of about 550 bags to 800 bags per hour.

Portals are capable of processing seven passengers per minute.

Vehicle screening detectors take approximately 1 minute.

User acceptance

Explosive detection units are noninvasive and carry no health concerns.

Vendors

The following vendors appear on the GSA schedule: Ion Track, Barringer Instruments Inc., SAIC, Raytheon, InVision Technologies Inc, L-3 Communications, Scintrex Trace Corporation, and Rapiscan.

Unit price range

A handheld device can cost between $20,000 and $45,000.

A tabletop detection device can cost from $20,000 to $65,000.

A portal system can cost from $80,000 to $400,000.

The largest baggage x-ray units are priced from $110,000 to $1.3 million. The medium size x-ray units for smaller packages range from $100,000 to

$235,000. Standalone units for personal belongings are priced from $30,000 to $50,000.

Attachment III: Intrusion Detection Technologies

Intrusion detection systems serve to alert security staff to react to potential security incidents. These systems are designed to identify penetrations into buildings through vulnerable perimeter barriers such as doors, windows, roofs, and walls. These systems use highly sensitive sensors that can detect an unauthorized entry or attempted entry through the phenomena of motion, vibrations, heat, or sound.

Closed circuit television (CCTV) is an integral part of intrusion detection systems. These systems enable security personnel to monitor activity throughout a building. Intrusion detection technologies can also be interfaced with the CCTV system to alert security staff to potential incidents requiring monitoring.

When an intrusion is sensed, a control panel to which the sensors are connected transmits a signal to a central response area, which is continually monitored by security personnel. The sensor-detected incident will alert security personnel of the incident and where it is occurring. By interfacing these technologies, security personnel can initially assess sensor-detected security events before determining how to react appropriately.

Attachment III--Intrusion Detection Technologies: Closed Circuit Television

Closed Circuit Television (CCTV)

Analog CCTV surveillance system.

Source: Pittway Corporation.

Vandal-proof dome camera.

Source: North American Security Solutions, Inc.

How the technology works

CCTV is a visual surveillance technology designed for monitoring a variety of environments and activities. CCTV systems typically involve a dedicated communications link between cameras and monitors. Digital camera and storage technologies are rapidly replacing traditional analog systems.

CCTV provides real-time or recorded surveillance information to help in detecting and reacting to security incidents. A CCTV system can also be used to prevent security breaches by allowing remotely stationed security personnel to monitor access control systems at entry points to secure areas. Other advantages to using CCTV include deterring criminal activity, promoting a safe and secure work environment, enhancing the effectiveness of security personnel, discouraging trespassing, providing video evidence of activities occurring within the area, and reducing civil liability.

A CCTV system involves a linked system of cameras able to be viewed and operated from a control room. Cameras come in two configurations: fixed made or pan-tilt-zoom mode. In pan-tilt-zoom mode they can either automatically scan back and forth or be controlled by an operator to focus on particular parts of a scene.

Some systems may involve more sophisticated technologies such as night vision, computer-assisted operation, and motion detection systems. A camera that is integrated with a motion detection system would, for example, enable alerted security staff to remotely investigate potential security incidents from a central control center. Other sophisticated CCTV systems incorporate technologies that make possible features such as the multiple recording of many cameras, almost real-time pictures over

telephone lines, low-light cameras, 360- degree-view cameras, the switching of hundreds of cameras from many separate control positions to monitors, immediate full-color prints in seconds from a camera or recording, and the replacement of manual controls by simply touching a screen. CCTV is also sometimes used to capture images for a facial recognition biometric system.

Effectiveness

The clarity of the pictures and feed is often excellent, with many systems being able to recognize a cigarette packet at a hundred meters. The more expensive and advanced camera systems can often work in pitch-blackness, bringing images up to daylight level.

However, CCTV systems are not considered to be suitable for high-security areas that require security staff to be present at entry control points. Also, inattention to monitors by security personnel, as discussed below, is a common problem.

Performance factors

The biggest problem concerning CCTV is proper installation. Since cameras vary in size, light sensitivity, resolution, type and power, it is essential to understand the target area before procuring a camera. Important aspects to be considered are lighting, environment, and mounting options. Because insufficient attention is often paid to all of these aspects before products are selected and installed, many CCTV systems do not work properly. Just how important proper lighting is is reflected in the Defense Protective Service's having installed 98 percent of their CCTV cameras in well-lit areas.

While CCTV can be used to supplement and reinforce security staff, using CCTV as an active surveillance tool is often not effective. Studies have shown that because monitoring video screens is both boring and mesmerizing, the attention span of a person watching and assessing a CCTV monitor degrades below acceptable levels after 20 minutes. CCTV is more effective when used, for example, at control points to actively allow or disallow individuals through a particular door on the basis of the security staff's recognition of the CCTV image of the individual.

Most CCTV systems have all their connected cameras record continuously. The result is an abundance of video material that must be manually reviewed if an incident that cannot be narrowed down to a particular time is being investigated. However, by using cameras that are triggered to turn

on by the occurrence of motion within their field of view, the amount of video that is recorded is greatly reduced and facilitates faster searches.

Whereas analog storage is space consuming and human intensive, digital technology allows large amounts of data to be captured, compressed, recorded, and automatically stored and managed so that recorded events can be tracked and located by date and time.

User acceptance

CCTV has raised much concern over privacy issues. Apprehensions are generally based on a fear that CCTV will be used for purposes other than for which they were intended. Examples of these concerns are that CCTV systems:

- may be used to monitor an individual's actions in real time or over a period of time;
- may be used by employers to monitor employees' performance, including when they arrive and leave work;
- may enable security personnel to indulge in voyeurism by especially focusing on attractive individuals; and
- may be used to arbitrarily monitor individuals of a particular race or ethnic background.

Apprehensions such as these have hindered organizations from exploiting the full potential of CCTV towards enhancing security. The Capitol Police, for example, does not plan to install many more cameras in its internal spaces because of the sensitivity of its members to internal surveillance.

Vendors

The GSA schedule lists the following CCTV vendors: Panasonic Security Systems Group, Extreme CCTV Inc., Ultrak Inc., and Silent Witness Enterprises Ltd.

Unit price range

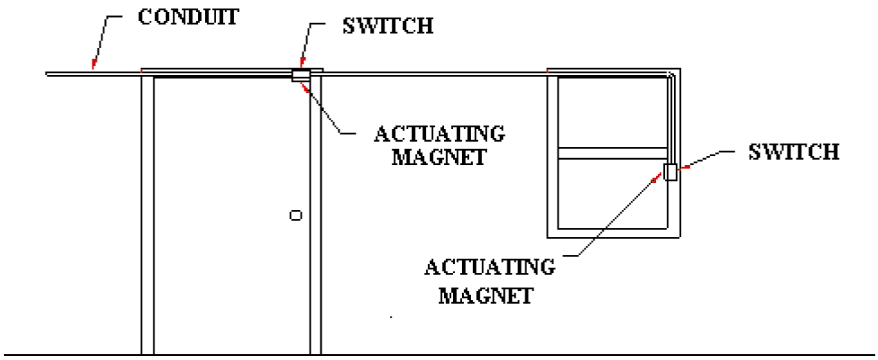
A fully integrated CCTV system for physical access surveillance can cost from $10,000 to about $200,000, depending on the size of the entrance and the degree of surveillance required for monitoring the area. For additional CCTV equipment, cameras can cost about $125 to $500. Cameras with advanced technological features can cost up to $2,300. Monitors can cost between $125 and about $1,000. Recorders can cost between $400 and $2,700, and a video control system (remote controller and accessories) between $3,000 and $12,000.

A 16-camera view of digital CCTV surveillance.

Source: Silicon Technologies, Inc.—Window Vision (c) 2002.

Attachment III—Intrusion Detection Technologies: Intrusion Sensors

Intrusion Sensors



TYPICAL BALANCED MAGNETIC SWITCH INSTALLATION

Source: National Institute of Justice.

How the technology works

Electronic intrusion detection systems are designed to detect penetrations into secured areas through vulnerable perimeter barriers such as walls, roofs, doors, and windows. Detection is usually reported by an intrusion sensor and announced by an alarm (typically to a central response area). The intrusion alarm must then be followed by an assessment to determine the proper response. CCTV is typically used in internal assessments to determine the validity of the alarm.

A variety of technologies have been developed for the detection of intrusions:

Line sensors use cables that are either placed above ground or buried in the ground. When positioned just outside a building wall, they can detect both prowlers and tunneling activity. Some lines are sensitive to magnetic or electric disturbances that are transmitted through the ground to the sensing elements, while others respond to changes in pressure from an intruder's footstep or vehicle.

Video motion detectors transform the viewing-only ability of CCTV cameras into a tracking and alarm system. By monitoring the video signals, the sensors detect changes caused by the movement of an object within the video's field of view. Sometimes only a portion of the total field of view is monitored for motion. The size of the moving object or its speed (for example, blowing debris or a flying bird) can sometimes be used to distinguish a person from other objects in motion.

Balanced magnetic switches are an extension of the conventional magnetic switch used on doors and windows in a home security system and are widely used to indicate whether a door is open or closed.

Conventional magnetic switches can be defeated by placing a steel plate or magnet over the switch, allowing the door to be opened while keeping the switch closed. Balanced magnetic switches activate an alarm if this defeat tactic is used.

Sonic and vibration sensors detect intrusion indicators such as the sound and movements of breaking glass or wood at windows and walls. Because they are typically used in rooms during timeframes when legitimate access is not expected, these sensors can also be used to detect the motion of a person walking into or within a designated area. While changes in sound waves are typically detected by sonic sensors, vibrations are typically detected by the use of microwave radiation or infrared (IR) light (both of which are invisible to the naked eye). Microwave sensors generate a detection zone by sending out a continuous field of microwave energy. Intruders entering the detection zone cause a change in this field, triggering an alarm. IR technology operates in two methods:

1. **Active IR sensors** inject infrared rays into the environment to detect changes. They generate an alarm when the IR light beam (similar to that used in a TV remote controller) is broken. Multiple active IR beams are often used at gates and doors to create a web of rays that make the system more impenetrable.

2. **Passive IR sensors**, also known as pyroelectric sensors, operate on the fact that all humans (and animals) generate IR radiation according to their body temperatures. Humans, having a skin temperature of around 93 ° F, generate IR energy with a wavelength between 9 and 10 micrometers. Passive IR sensors are therefore typically set to detect a range of 7 to 14 micrometers.

Effectiveness

Sensor technology has been relied on for many years as an effective countermeasure to security breaches. However, this technology is susceptible to nuisance alarms or false alarms not caused by intruders. Depending on the technology used, disturbances that contribute to nuisance alarms can be generated by animals, blowing debris, lightning, water, and nearby train or truck traffic. Nuisance alarms can be mitigated by adjusting a sensor's sensitivity level and by careful routing of signal cables.

Performance factors

Because these intrusion detection systems operate on electricity, any disturbance in the electrical power will affect their performance. Special

design considerations must be given to the routing and protection of power and signal cables to prevent exposure to tampering and environmental wear and tear.

Careful placement of sensors is also critical to their success. Some vibration sensors should not be mounted directly on window glass, as the mounting adhesive may not be designed to withstand long exposures to heat, cold, and condensation. Because passive IR sensors detect changes in temperature, their sensitivity would decrease if placed in rooms that would approach the same temperature as the human body. Manufacturers' specifications for each sensor technology should be heeded to ensure maximum performance.

User acceptance

Doors and windows that have been equipped with intrusion detection devices cannot be propped open for circulation of fresh air. A building with a large number of windows cannot be fully secured with an intrusion detection sensor unless all windows are equipped with the devices.

Vendors

For the technologies discussed above, The National Institute of Justice's *Perimeter Security Sensor Technologies Handbook*[1] lists the following vendors: ADT Security Systems, Advantor, DAQ Electronics, Detection Systems, Inc., GYYR, Microwave Sensors, Millennium Sensors, Presearch, Safeguards Technologies, Scantronic, Senstar, South West Microwave, Stellar Security Products, Vindicator, and Visonic LTD.

Unit price range

Line sensor cables range from about $300 to $750 for 100 meters. Line sensor detection systems are available for about $1,000.

Video motion detector cameras range from about $150 to $1,500.

Balanced magnetic switches range from about $100 to $289.

Simple microwave sensors are available for about $30, while comprehensive microwave detection systems range from about $400 to $1,000.

[1] *http://www.nlectc.org/perimetr/full2.htm*

Infrared sensors range from about $25 to $200.

(310125)