J O U R N A L O F

DEFENSE & DIPLOMACY

Vol. 5 No. 8 1987, $3.50

The Magazine of World Leaders

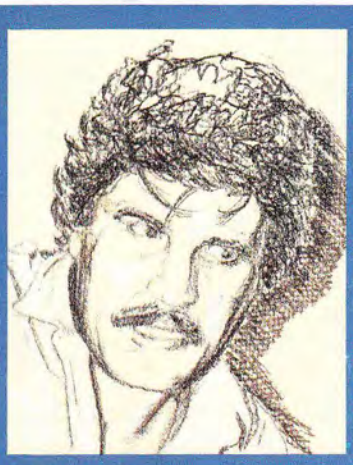
JAPAN'S SELF-DEFENSE FORCES

A REMOTE-CONTROLLED MINE SWEEPER

1987 PARIS AIR SHOW REPORT

New Zealand Security

Networking for Power and Protection



Eyedentify Counters Security Threat

By Barry Becker

High-level crime, terrorism and industrial and political espionage costs billions of dollars each year and jeopardizes invaluable intelligence assets. Security is a pervasive concern today for companies and government agencies, as well as individuals. Growth in crimes against individuals often is matched or exceeded by increases in crime against corporations or governments. Traditional security methods such as locks, codes, identification badges and guard stations are no longer effective in providing the high level of security that many installations require today.

One particularly vulnerable area of security is positive identification. Passports and badges can be altered or duplicated. Locks and codes can be broken. Guard stations can be overtaken. It may even be possible to tamper with an individual's fingerprints.

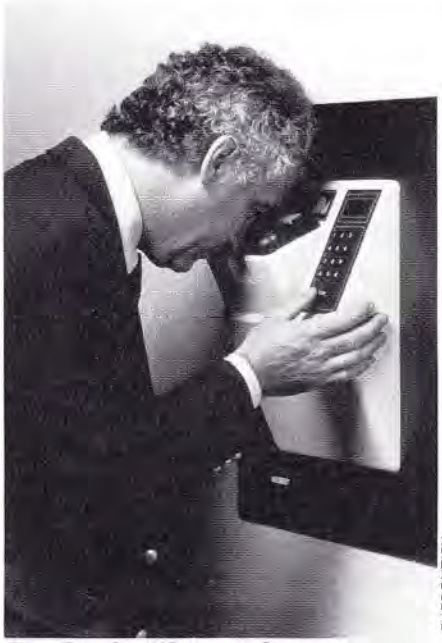
But positive identification problems have been answered by a new technology: biometrics. The process revolves around a variable which is virtually impossible to lose, steal, duplicate or forge—the pattern of blood vessels in the retina of the human eye.

Access Threatens Security

Security has always been a concern for people, companies and governments, but the intensity of that concern has risen in recent years. This is due to several reasons.

First, crime in general is increasing, and the proliferation of worldwide terrorism has shown that some groups will stop at nothing to attack the people and property of a disliked nation or organization. The facilities of large corporations, utilities and government agencies have increasingly become targets for disruption and sabotage.

Second, the widespread use of computers has left vast amounts of critical information at the mercy of persons able to crack computer-access safeguards. Traditional methods of security access are proving inadequate. Passwords and code numbers can be copied or accidentally revealed, cards and keys can be lost or duplicated, and individuals can be coerced into signing in a "visitor." For example, one terrorist group used an American serviceman's identification card to gain access to a military base in West Germany before setting explosive charges to knock out a utilities target.



EYEDENTIFY

The Eyedentify security access system.

For these and other reasons, positive identification has become a critical consideration for government agencies and businesses. Most security needs boil down to one goal: to ensure that no unauthorized person gains access to particular areas or information.

Security access is commonly divided into three levels. Qualified access is the lowest level. At this level, a person qualifies for access based on possession of an item or piece of information—a key, card or code number. No attempt is made to ascertain the individual's identity. The second level is verified access. Here, some check is made to verify the identity of the person presenting credentials. For example, a guard might compare the picture of an ID badge with the person wearing it. (In congressional hearings, one convicted spy stated that he deliberately placed a picture of a gorilla on his photo badge, and still gained access.) Positive identification, which provides absolute assurance of an individual's identity through a fool-proof method, is the highest level of security. A 1982 study by the research firm Frost and Sullivan indicated that a majority of security directors and business and government officials were dissatisfied with the protection offered by the lower two levels of security, and were seeking other means of positive identification.

Biometrics to the Rescue

Perhaps the most promising area for achieving positive identification is biometrics. Simply put, biometrics is a means of identifying a person by examining a particular physical characteristic. A biometric security system works on the principle that a machine must positively identify a person by recording the necessary characteristic and comparing it to a library of characteristics belonging to the people qualified to gain access. Among the characteristics used for this purpose are fingerprints and lengths, voice patterns, handwriting style and retinal patterns.

A retinal-scanning system has two broad advantages over the traditional identification methods and other biometric techniques. First, a person enrolled in such a system does not have to carry, remember or present anything but himself/herself to gain access. Second, because no external device or memorization is required, the critical variable in determining access cannot be lost or transferred. This system is the only biometric security-access product that does not require a corroborating personal identification number. Eyedentify, Inc., of Portland, Ore., manufactures the patented Eyedentification System 7.5 which can be used as a stand-alone to protect one door with bubble memory capacity for 1,200

Barry Becker is the vice president in charge of international marketing for Eyedentify, Inc., Portland, Ore. He moved to the company after seven years in the consumer electronics field, and he was formerly a vice president of Insoft, Inc., a computer software company.

network of units reporting to a host computer or existing security system. The Eyenet System 8600 is a dedicated system of eyenet "reader" units that can expand up to 32 units with an SDLC loop configuration to an Eyenet controller (a bubble memory residing in the controller with a capacity of 1,800 eye signatures).

Retinal-scanning technology is based on the fact that no two persons have the same pattern of blood vessels in their retinas. Awareness of this characteristic goes back to 1935 when Dr. Carleton Simon and Dr. Isodore Goldstein published a paper on the use of retinal photographs for identifying people based on blood vessel patterns.

Two decades later, their conclusions on the uniqueness of retinal patterns were supported by Dr. Paul Tower in the course of his study of identical twins. Of any two persons, identical twins would be the most likely to have similar retinal vascular patterns. Tower's study, however, showed that of all the factors compared between twins, retinal vascular patterns showed the least similarity. Although other physical retinal features are unique to individuals, none are as stable as the retinal vascular pattern. The eye shares the same stable configuration as the brain, and only a small number of diseases or serious physical injuries can alter the blood vessel patterns of the retina. Such diseases and injuries are relatively rare, making the retinal pattern an extremely useful and reliable method of biometric identification.

Retina-Scanning Quick, Easy

The retina-scanning procedure starts with a 450-degree circular scan of a portion of the retina centered on the fovea, the area of sharpest vision. The machine requires the subject to look into a viewfinder eyepiece and focus on a series of green dots. Once the dots condense into one green dot, the subject is properly aligned and in focus, and the scan button is initiated. A low-intensity infrared light is used by a camera (called the ICAM) to make the retinal scan. As it scans the fovea, the ICAM camera takes 320 readings, measuring variations in reflection which indicate the pattern of blood vessels. A software-implemented phase corrector compensates for rotations of the head or eye. The focusing and scanning requires only about two seconds for verification. The scan by the ICAM produces a waveform which is converted into digital impulses and sent to a microprocessor. In the enrollment mode, the digital retinal pattern is converted into a 40-byte template that is stored in memory.

Normally, only the right eye of a user is examined. Both eyes can be enrolled, however, if a greater level of security is desired, or the system can be used to enroll two persons under one template. The latter method is used in situations where security dictates that two persons enter an area together. When used in this dual-enrollment fashion, the Eyedentify system prevents an unauthorized person from posing as one half of a team.

Accuracy and Safety

In the fictional James Bond movie *Never Say Never Again*, the "bad guy" duplicates the U.S. president's retina and gains access to nuclear cruise missiles. In the real world, such a scenario is virtually impossible to accomplish because the individual has to make a "brain-retina" decision and determine when his or her eye is in focus, and because the system has a mechanism to detect the difference between a glass eye and a real eye.

The accuracy of biometric devices is accessed through the measurement of its false accept rate. Acceptance of a person who should be rejected is of great concern to the user of a high-security system. Testing of the retinal-scanning technology has shown the false accept rate to be one false acceptance in a million, using the threshold setting at .71 percent in one eye. To increase the false acceptance rate significantly, one must increase the threshold and/or enroll two users. In 1984 a semi-government research company that works with the U.S. Department of Energy tested the Eyedentify system and found that it had a zero false accept rate. Toyo Engineering Co. of Japan conducted an evaluation test that consisted of 770 people in their control group and claimed that Eyedentify had a zero false acceptance rate.

Safety is, of course, a natural concern whenever eyes or vision are discussed. The retinal-scanning system poses no risk whatsoever of physical damage or disease. The levels of infrared light emitted by the ICAM during scanning are several magnitudes below the safety levels established by the American Conference of Governmental and Industrial Hygienists and recommended by the U.S. Food and Drug Administration (FDA). The University of Washington's ophthalmology department and Oregon Health Science University's chairman of the Department of Ophthalmology stated that the Eyedentify retinal-scanning technology is perfectly safe to users' eyes. The Swedish Institute of Radiation also tested the system and came up with the same results—perfectly safe.

Modern security techniques for manned missile sites have improved the ability to detect an adversary. Automatic response systems will do things like turn on lights and alarms, lock doors, pour out sticky foam or smoke and drop a concertina wire mesh to immobilize an intruder. Foreign governments go even further; the intruder might hear the announcement: "You are in the middle of a mine field, do not move."

In the interests of protecting governments' invaluable assets, security officials are implementing an arsenal of security to detect, neutralize and, if necessary, terminate intruders. The U.S. Air Force employs four levels of security: card identification, personal ID number and the Eyedentify system, as well as a device that automatically computes body weight while the user is dealing with the other security measures. Other organizations that employ the Eyedentify retina-scanning system include the Departments of Defense, Energy, Justice and the Kennedy Space Center.

Positive identification in high-level security environments is crucial if governments and businesses intend to seriously reduce the terrorist threat worldwide. How many government security officials can be certain that the person claiming to be an authorized official wishing to see a top political figure is in fact the right person? How many security officials rely on the mere possession of a card or knowledge of a password as the established criteria to admit a person or persons into a sensitive area that stores government or business secrets, weapons, information, monies or chemicals? The time is drawing near for security professionals to seriously move ahead and demand systems for positive identification.