U.S. military looks to biometrics for security. (Special Report).
John McHale

12/01/2002
Military & Aerospace Electronics
14

U.S. Department of Defense officials are focusing on **biometric** solutions--facial recognition, iris recognition, and fingerprint recognition--to help secure their facilities worldwide. Meanwhile, facial-recognition systems are becoming a familiar site at airports across the country.

Since the terrorist attacks of Sept. 11, 2001, the global war on terrorism has brought increased focus on **biometric** technology as a security solution for identifying and tracking suspected terrorists and criminals at airports, sporting events, nuclear power plants, and other high-profile facilities.

The war on terrorism has now increased the focus and spending on **biometrics** technology for the military. The current DOD budget contains more than $200 million for facilities security worldwide, says Phil Hamilton, a vice president of Curtiss-Wright in Littleton, Mass., a good portion of which is going to go toward **biometric** technology, he adds. Curtiss-Wright produces a combined iris-, hand geometry-, and facial-recognition system for the military and commercial sectors.

"As a whole, the military departments are working with all of the more mature technologies (fingerprint, iris, hand geometry, and face) to determine where each might be most applicable," says Steve Bertocchi, program manager for the DOD **Biometrics** Management Office (BMO) at the Pentagon. "The success and effectiveness of the technology really depends on the system. Fingerprint is the most mature as it has been around the longest, and can usually be purchased at a lower cost than other **biometrics**. Iris is considered by many to be the most secure."

The BMO understands the benefits of leveraging commercially available technologies and has focused the majority of its resources on COTS (commercial-off-the-shelf) products, Bertocchi points out. "That said, the BMO has left open the option of developing government-specific solutions, but will only do so if the potential benefits outweigh the costs," he says.

Common Access Card

One of the biggest **biometric** programs for the DOD is the Common Access Card program, otherwise known as CAC, which involves putting **biometric** technology on a new smart ID card.

A smart card is a credit card-size device that contains one or more integrated circuits and may also employ one or more of the following technologies: magnetic stripe; barcodes, linear or two-dimensional; non-contact and radio frequency transmitters; **biometric** information; encryption and authentication; or photo identification.

"The Common Access Card is the first DOD-wide implementation of smart card technology," says Jim Lynch, program manager of the CAC/Public Key Infrastructure (PKI) at Maden Tech Consulting Inc. in Arlington, Va. The PKI component of CAC uses encryption and digital signatures to safeguard information, he says.

The CAC has five primary functions:

* replace the existing DOD identification card;

* identify active-duty military personnel (to include the Selected Reserve), DOD civilian employees, and eligible contractor personnel;

* give physical access to buildings and controlled spaces;

* allow computer network and system access; and

* authenticate the Public Key Infrastructure.

"Retirees and military dependents will not receive the CAC, but will continue receiving the current identification card, Lynch says.

"With a CAC application, many paper-based processes will become automated, therefore, what may have taken days to do may now take just hours," Lynch continues. "Military Service members may use the CAC to enter their installation, log onto computers, or verify medical benefits eligibility, or gain dining facility privileges. As the technology matures, the CAC will perform even more Functions, thereby enhancing readiness and saving time and money for all personnel.

"PKI supports specific functions such as secure single sign-on access control, digitally signing electronic documents, and encrypting e-mail. Eventually, all DOD computers will have a card reader allowing network access using the CAC. PKI adds an extra layer of security, because without your CAC, no one can log onto your computer even if they have your name and password. PKI authentication also provides the DOD another weapon to foil the attacks of computer hackers on DOD computer systems. With PKI, personal privacy is better protected and national security is also strengthened."

Smart card technology may streamline business processes, as well as help share and protect information, Lynch explains. "For instance, because smart cards can securely store and carry information about military personnel, organizations can minimize paper-based, labor-intensive processes, thus saving money and time," he says. "Additionally, because smart card technology supports multiple applications on one platform, the number of cards issued to service personnel will be reduced."

Enterprise solutions

DOD and industry experts are looking at ways to combine the benefits of separate **biometric** solutions such as face, fingerprint, and iris into one enterprise solution.

"The **Biometrics** Management Office recently introduced the **Biometrics** Enterprise Solution, which helps the DOD perform trusted sharing of a person's **biometric** credentials between

authorized entities," Bertocchi says. "This approach will support DOD-wide identification and authentication requirements and will be integrated into DOD's current business processes.

"Working groups have been chartered to address each of the four key areas of the solution -- collection, repository, access and retrieval, and use," Bertocchi says. "Each of these working groups consists of key stakeholders including the BMO staff and DOD Services and Agencies. As the DOD Executive Agent for **biometrics**, the BMO has established a **Biometrics** Senior Coordinating Group to oversee, provide guidance, and make decisions relevant to the DOD **Biometrics** Enterprise Solution."

Two companies--Curtiss-Wright, as well as Inforonics in Littleton, Mass.--are teaming on an electronic system able to combine several forms of **biometric** analysis for government, military, and commercial security.

Any technology that analyzes fingerprints, eye retinas, eye irises, voice patterns, facial patterns, or hand measurements may be impressive by itself, but is not infallible, points out Adam Albina, manager of software development at Inforonics. Combining them in one networked solution with a continuously updated database increases efficiency, he explains. By company agreement, Inforonics blends separate **biometrics** solutions and Curtiss-Wright licenses **biometric** technologies.

Enterprise solutions are the hot topic right now, Curtiss-Wright's Hamilton says. Designers, government, and industry alike recognize it is the best way to provide security, he adds.

Curtiss-Wright experts are also working with TRW in Redondo Beach, Calif., and Northrop Grumman in Los Angeles to demonstrate **biometric** solutions for the U.S. Air Force under the Leap Ahead program, sponsored by the Air Force Electronic Systems Center at Hanscom Air Force Base, Mass., Hamilton says.

Air Force officials are particularly interested in a two-man trapped system for weapons facilities, he says. Two personnel would enter a controlled room, each by using hand geometry and a smart card for the first door of the control room. Then they provide hand geometry, smart card identification, and facial recognition to get through the second door, Hamilton explains.

The Curtiss-Wright technology was also part of the Leap Ahead program in Northrop Grumman's Smart Gate solution at a U.S. military base in San Diego, Hamilton says. The entrance gate to the base is electronically set up to recognize license plates, smart cards, and **biometrics** to provide identification based on the current level of threat, he explains. "If the threat is low only the license plate will be used for identification," Hamilton continues. "However, if the threat is high, **biometrics** such as face and hand geometry will be used," he says.

Curtiss-Wright is licensing a facial-recognition system from Viisage Technology, a subsidiary of Lau Acquisition Corp., in Littleton, Mass., Hamilton says. Curtiss-Wright also produces sensors and other electronics applicable to **biometrics** security applications in military, aerospace, and nuclear power, Hamilton says.

The new solution from Curtiss-Wright and Inforonics eases the movement of authorized personnel, while keeping out intruders, Albina says. It can foil **spoofing** attempts by blending facial, voice, or hand recognition, Albina says

It also can record **biometric** data from intruders and update worldwide law-enforcement databases over secure Internet connections in real time, he says. Today, government agencies, airports, and companies can wait weeks for mailed CD-ROM data updates, Albina says.

It keeps crucial information out of the wrong hands by using either a virtual private network over Internet Protocol (IP), or with the IPSec security Internet protocol of the Internet Engineering Task Force, Albina explains.

The so-called "**Biometric** Intelligence Solutions" from Inforonics seamlessly integrate **biometrics** systems from separate vendors on the Enterprise **Biometric** Framework (EBF) -- the core architecture of Inforonics's **biometrics** -- says Dave Gabree, vice president of client services at Inforonics.

The EBF development environment enables **biometrics** applications programmers "to quickly and easily implement application logic that performs a variety of **biometric** functions including sample capture, **biometric** template production (enrollment), identification, and verification," Gabree says. Functions use the industry-standard BioAPI version 1.1 interface, he adds.

The EBF, a simple interface to low-level functions of proprietary **biometrics** systems, provides functionality "that normally would require a series of complicated application program interfaces (API)," Gabree says. The initial EBF uses Viisage software's ability to acquire images, generate Eigen coefficient vectors, and compare Eigen vectors stored in the database.

Airport security

Facial-recognition technology is also becoming more and more a fixture at airports nationwide. Viisage officials claim their facial-recognition technology has worked successfully in passenger screening tests at airports around the country.

"We have had a success rate in excess of 90 percent," says Cameron Queeno, chief marketing officer for Viisage. "I feel safe letting my wife on a plane with that type of efficiency," he adds.

Some of tests are still going on, such as the one at Logan airport in Boston, and some airports are already installing facial-recognition systems such as Manchester airport in Manchester, N.H., Queeno says.

"We have learned a lot about facial-recognition technology since 9/11," Queeno says. "Most importantly in the way we deploy it, he adds. For example at tests before 9/11 at the Super Bowl and other facilities cameras would be set up to watch people as they are walking and record an image of their face to be crosschecked with a database, Queeno explains. However, because the people were not directed to look into the camera, the image is recorded were sometimes insufficient for recognition, he says.

Now facial-recognition systems are becoming part of the regular airport security check-in, Queeno says. When a passenger goes through security he first puts his luggage through the baggage-screening system, and then steps through the metal detector, Queeno continues. Now security personnel will ask him to look into a camera that will take his picture for the

facial-recognition system, which will take six impressions of his face then compare those to a database that would typically carry about 1,000 people labeled as suspicious or worse, Queeno explains.

Each passenger's face is usually erased unless he resists, or security personnel label his behavior as suspicious, Queeno says. If a passenger refuses to look into the camera, he is not allowed to board the plane, he adds.

If the operator of the facial-recognition system finds a match, he can alert security personnel to perform a more extensive search of the passenger or ask them just to observe the passenger in case he may make contact with someone else, but still detain him before he gets on the aircraft, Queeno explains.

"Facial recognition is a tool like baggage screening," Queeno says. Having passengers stop to look at a camera is easier than trying to pick them out of a crowd, he adds. Plus if someone is wearing a hat or trying to look away from the camera, they cannot get away with that when security is standing next to them, Queeno says.

The Viisage technology is also under consideration for law enforcement, Queeno says. For example, a police officer might pull someone over, use a handheld facial-recognition device to take his picture then plug into a laptop in the police cruiser to crosscheck the suspect's face against a national database, Queeno explains. There is also talk about creating a smart card for frequent fliers that contains their faces and fingerprints that would enable them to pass through the long security lines, Queeno says.

The Viisage family of face-recognition products includes FaceEXPLORER, an image retrieval and analysis database product, used to combat identity fraud; FaceFINDER, a surveillance and identification system currently used in casinos and at sporting events; FaceNET, which provides secure authentication for PC, Internet, and e-commerce connections; FacePIN, which provides private verification for point-of-sale transactions such as ATMs; FacePASS, a security solution for keyless entry to secure facilities, such as offices, dormitories, and government facilities; and Face-TOOLS, a leadership software developers kit that enables application providers the ability to develop and customize customer and market applications.

Viisage's FacePASS has been successfully installed and is now operating at the U.S. Navy San Diego Submarine Base in San Diego. Viisage is working with the Navy to integrate FacePASS into a mantrap environment that limits access to one person at a time and will enable the Navy to move from a manned facility to an unmanned facility, permitting access to the pier during off hours.

"Our initial findings have been promising," says Cindy Milholland, a project engineer for the Navy. "In the present environment, the system is performing the job of access control very well."

Company information

Company Location Phone

AcSys **Biometrics** Corp. Burlington, Ontario 905-634-4111

AXCESS Carrollton, Texas 800-588-60B0

Biometric Key Systems Richardson, Texas 972-998-0204

Curtiss-Wright Littleton, Mass. 978-952-2000

IDenticard Systems Inc. Lancaster, Pa. 717-569-5797

Inforonics Littleton, Mass. 978-698-6400

Iridian Technologies Moorestown, N.J. 856-222-9090

Northrop Grumman Los Angeles, Calif. 310-553-6262

Primagraphics Charlottesville, Va. 434-951-9460

Raytheon Arlington, Va. 703-284-4346

Secure Computing Corp. San Jose, Calif. 408-918-6100

Viisage Technologies Littleton, Mass. 978-952-2200

Visionics Jersey City, N.J. 201-332-9213

Company Web

AcSys **Biometrics** Corp. http://www.acsysbiometricscorp.com

AXCESS http://www.axcessinc.com

Biometric Key Systems http://www.biokeysys.com

Curtiss-Wright http://www.curtiss-wright.com

IDenticard Systems Inc. http://www.identicard.com

Inforonics http://www.inforonics.com

Iridian Technologies http://www.iridiantechnoiogies.com

Northrop Grumman http://www.northropgrumman.com

Primagraphics http://www.primagraphics.net

Raytheon http://www.raytheon.com

Secure Computing Corp. http://www.securecomputing.com

Viisage Technologies http://www.viisage.com

Visionics http://www.identix.com

RELATED ARTICLE: Raytheon and Visionics demonstrate facial-recognition system at Boston's Logan Airport

Engineers at Raytheon Co. and Visionics Corp in Jersey City, N.J., recently achieved a high rate of successful matches in field tests of a facial-recognition system at Boston's Logan International Airport.

Powering Raytheon's facial-recognition system was the Visionics FaceIt Argus System, deployed in a real-life setting at a security checkpoint where subjects were matched against a watch list.

"Based on the test results, Raytheon will be able to recommend approaches to using **biometric** tools to provide higher levels of security at U.S. and international airports," says

Ramsey Billups, Raytheon technical director of **Biometrics** and Secure ID Systems.

"The Logan Airport activity and results proved the viability of surveillance face-recognition technology," says Brad Hollenberg, Raytheon director of **Biometrics** and Secure ID Systems.

"Our state of the art technologies coupled with Raytheon's renowned domain expertise within airports together provides scalable and easy to deploy platforms that will support mass deployments across the globe," says Joseph Atick, chief executive officer of Visionics. The technology has also been tested at other airports around the country where several positive watch list identifications have already been made, Atick adds.

"We have made our airport available to the TSA as a proving ground for new technologies that can counter the new threats we are facing," says Sam Sleiman, Massport's deputy director of Aviation Design and Construction. "This program has the potential to be an important part of an overall security program."

Iridian iris-recognition system used at John F. Kennedy International Airport

Officials at New York's John F. Kennedy international airport are using iris-recognition technology from Indian Technologies in Moorestown, N.J., for a pilot program to prevent employee security breaches at the airport.

The iris-recognition system is installed in a door to the tarmac of Terminal 4, which is the international arrivals hall at JFK Airport, Indian officials say. The voluntary test program has so far enrolled 300 of the airport's 13,000 employees.

"By introducing the accuracy of iris-recognition to protect sensitive areas like the tarmac, stolen identification cards and compromised keypad access codes will no longer pose a significant threat," says Frank Fitzsimmons, chief operating officer of Indian Technologies.

The employee enrolls in the system by glancing at an iris-recognition-enabled camera, then the iris-recognition software converts a digital picture of the employee's iris into an IrisCode record, Indian officials say.

To proceed through the door to the tarmac at Terminal 4 the employee's identification card must match a live read of the person's iris, Indian officials say. If a card is presented, but the iris does not match the IrisCode record for that person, the door to the tarmac will not open. Security personnel are also dispatched to interview the individual and determine the next steps, which may involve local authorities. The Transportation Security Administration will monitor results, company officials say.

Iris-recognition technology identifies people by the unique patterns of the iris -- the colored ring around the pupil of the eye, Indian officials say. Indian's iris solutions examine mere than 240 degrees of freedom in the human iris to create the IrisCode record, a 512-byte data template used to identify individuals and/or authenticate user privileges, company officials say.

Iridian's Private ID technology includes camera drivers for IrisCode creation using standard video technology without bright lights or lasers, Indian officials say. KnoWho Authentication Server is Iridian's scalable server that provides interoperability for all private ID-enabled cameras and applications. This security solution ensures individual authentication against

millions of records, and is targeted for public-use applications such as border control or simplified passenger travel, company officials say.

AXCESS and AcSys **Biometrics** combine wireless and facial-recognition technology

Officials at AXCESS Inc. in Carrollton, Texas, are combining their wireless identification tags with facial-recognition systems from AcSys **Biometrics** Corp. in Burlington, Ontario, as a joint solution for access control applications.

The new partnership will create an access control solution with the accountability of **biometric** authentication and the convenience and speed of RFID (Radio Frequency Identification), AcSys officials say.

"We see the use of wireless tags as a key enabler for the acceptance of facial-recognition systems," says Allan Griebenow, president and chief executive officer of AXCESS. "They allow for automatic reading, without any presentation required by the user. By using a tag, you make it easy to manage the data for authorized users. And, you narrow down the comparisons the system has to make. The overall system works much faster. It also makes deployment on a grand scale feasible for large organizations, for the military, and for government."

"By strategically positioning ourselves with AXCESS Inc., who provide key enabling technologies in both video compression and RFID solutions, we feel we are one step closer to our goal of providing the ultimate in secure and user-friendly identity authentication solutions for today's enterprise," says Jerry Janik, President of AcSys **Biometrics** Corp. AcSys **Biometrics** is a joint venture between NEXUS Group International Inc. and AND Corp., the inventor and developer of Holographic/Quantum Neural Technology (HNeT), which is the technology behind the company's facial-recognition systems.

The combined system provides the accuracy and speed of "one-to-one" **biometric** verification with the convenience of "one-to-many" **biometric** identification, AcSys officials say. In "one-to-one" mode, a user claims an identity -- usually by presenting a swipe or proximity card. Then the **biometric** system authenticates a **biometric** sample -- such as a facial image -- against the **biometric** template on record for the claimed identity. Because the system only has to examine one template, identity authentication is fast and accurate, company officials claim.

In "one-to-many" mode, the user does not claim an identity and the **biometric** system has to compare the **biometric** sample against all templates on record in order to find a match, AcSys officials say. This process is necessarily slower (particularly if the database of users is large) and less accurate (because the chance of a false positive is higher), company officials say.

The AXCESS wireless identification tags automatically present a user's identity for authentication when the user approaches the access control point, AcSys officials say. In addition, the AXCESS tag system can be used to locate people automatically after they have entered the facility. The two systems are linked together with a standard communications interface, company officials say.

The AXCESS' Active Tag RFID product uses small, battery powered tags, which when automatically activated at control points throughout a facility, transmit a wireless message, typically as far away as 30 to 100 feet.

The combined solution also includes the AXCESS wireless video transmission system for handheld computers, which provides immediate notification of breaches, AcSys officials say. A video/audio transmitter sends key data about failed attempts to the pocket PC via wireless local area network. Live and recorded video and audio are available to notify key personnel immediately and enable rapid response. The receivers can use a wireless connection to the existing corporate network, or connected serially, or via the industry standard Weigand interface to other security systems, company officials say.