



Consulting • Systems Integration • Outsourcing
Infrastructure • Server Technology

A secure scenario — layered integration of biometric-based identification

Ed Schaffner – Director,
Positive identification and access control solutions

White paper

A decorative graphic consisting of several overlapping, thin, red circles of varying sizes and positions, creating a sense of depth and movement. The circles are centered around the word "secure".

secure

Layering biometric identification technologies can create a more secure information system or critical infrastructure.

Keeping them out

Why can't we keep the terrorists out of our country, off our airplanes, away from our mail, nuclear plants, power grids, food and water supplies? With all the technology available today, why can't we identify the bad guys in time to stop them? Before we can stop them, we have to know who they are and what they're doing. That's not an easy task.

Threads of information from a wide range of sources must be pulled together and analyzed. Each clue must be checked, associations and behavior patterns analyzed, and identities established. Today, the technology exists to mine the information from multiple databases across boundaries. Discussions are underway at the highest levels of our government to increase access to these databases for the purpose of analyzing activities and associations by known or suspected members of terrorist groups. Once faces are associated with the names, a variety of identification solutions at various access points can assist our security forces with identification, surveillance and arrest.

A lot of recent press has focused on the application of face recognition technology in airports and public buildings. Used appropriately, face recognition solutions can be very powerful tools in the fight against terrorism. Technology can continuously scan a crowd, comparing each face to those in the database and alert security personnel that a face resembles someone tagged in its database. That's where the automation stops and human intelligence must take over for final identification. The same holds true for other identification technologies used to combat terrorists.

Voice, fingerprints, hand geometry and iris recognition technologies combined with human reasoning and decision-making skills can be extremely powerful tools.

Identification and integration

The crux of the problem is pulling it all together — the identification technologies and their integration into databases and applications from various agencies. Integration — so that associations can be assembled and identifications made. And stronger protection afforded our critical infrastructure.

Finding the right solutions

We will never be able to eliminate the threat, but we can take steps to manage our risks. The first and most important aspect of providing protection to critical infrastructures is gaining an understanding of the entire picture. What resources need protection? What is the value of those resources? What will it take to replace them? What impact would loss have on the business, the economy or on the lives of those who depend upon them? What are the risks and the vulnerabilities?

A vulnerability assessment that thoroughly analyzes the environment, the needs, the risks, the threats and the impact of disruption is a critical first step.

The second step is developing an action plan and taking steps to implement process changes or technical solutions. Quite often, controlling access to the facilities and networks ranks highest on the list of improvements needed. Various vendors of biometric solutions are claiming world leadership positions with their solutions. This press has drawn significant attention to the technology and to the companies.

However, many projects have met with less than favorable results because a thorough understanding of the business case, the operational environment and the business process was not considered before a solution was implemented. No single biometric technology can cover all the bases and no single product can outperform its peers in all environments or business cases.

Let's go back to our face recognition discussion. To determine which face recognition solution to use you need to know how much control of the environment you have. Some solutions require near lab-like environments and very cooperative participants for optimum performance, while others can accommodate a wider range of operational conditions.

Caution should be exercised when working with vendors or suppliers who are devoted to one technology or one solution. There is no "Access Control for Dummies" guide for security managers or IT shops to help guide you through the selection process.

Do your homework before selecting the solution you believe meets your specific needs and try a small pilot before committing. Better still, work with an experienced integrator that has a proven process for analyzing the business needs and environment with no preferred or exclusive arrangements with specific technologies or vendors. You want the technology that best meets your business needs, not the technology recommended by the guy with one club in his golf bag. What is the ideal solution? The answer falls back to the vulnerability assessment and recommendations.

Unisys — Positive identification and access control

Unisys is working with a number of universities, companies and customers to integrate leading-edge enhancements to improve recognition solutions for access control at our borders, our airports, and to our infrastructures that support transportation, banking and finance, communications, power grid and government services. As an integrator, combining these advancements in technology to meet specific business needs offers interesting challenges and exciting opportunities — to prevent unauthorized access, reduce the need and costs for physical entry control personnel and helpdesk support. Partnering with our customers, vendor-suppliers and talented engineers across the company helps us to turn the visions of today into the realities of tomorrow. A safer, more secure world.

Here's a scenario using layering and integrating these technologies — all available today — that might provide protection for a nuclear power facility.

An example of layered integration — a secure scenario

Let's take a look at some of the high-tech solutions that are available today in the context of a scenario providing protection for a nuclear power production facility. How can security personnel detect the presence of a threat in order to counter and manage the associated risk? What steps can be taken to control access to the grounds, the building, the office, the information system and specific software applications?

A layered defense, starting at the perimeter is needed — one that integrates information from various types of sensors with information stored in databases to provide early warning to security personnel and afford flexible protection with no single point of failure. Remote detection devices such as video surveillance cameras with zoom lenses, coupled with motion sensing and automatic tracking software, can detect and track small movements hundreds — to thousands — of yards away depending on the quality of the optics. Pattern recognition software can be trained to recognize practically any object in the camera's field of view. Sensitive microphones and seismic sensors can detect sounds and vibrations at long distances. Smart fences can be used to detect a person walking six feet away from the fence.

Using similar technology, chemical, biological and radiation sensors can detect trace amounts of a wide range of agents. Computers interpret the data from the sensors and automatically control the air-handling system to dissipate or contain any agents so that inhabitants are protected as best possible. Doors close, doors open, windows close, windows open, air handling units shut down, open up — whatever is required. Sound far fetched? The FBI building supporting the Olympics in Salt Lake City was equipped with this technology. It is all available. Today.

Powerful optics mounted on a surveillance camera coupled with the latest generation of face recognition software, enable someone to be identified at long distances if they have been “enrolled” in the system. Audio sensors with voice recognition software can be used to identify voices. R&D is underway that will enable face recognition software to improve the ability to identify individuals from 2D photographs with surprising accuracy. R&D in 3D imaging is underway that will significantly enhance the accuracy of face recognition technology. Similarly, other projects are underway to improve the accuracy of voice recognition and filter out background noise to enable the listener to understand what the individual is saying.

A vehicle approaches — controlling access to the perimeter

As a vehicle approaches the entrance of our compound, a camera quickly scans it and pattern recognition software compares the information in the photograph to its database to determine the make and model. Similarly, another camera zooms in on the license plate. The combined information is compared to that on file for vehicles authorized to be on the property. A camera supported with face recognition technology does one final scan of the driver to determine if he or she is the driver of record for the vehicle, or otherwise authorized to be on the property. Assuming the system has validated the vehicle and the driver, the gate is opened. If at any point the information in the database does not support the claimed identity of the vehicle or its driver, entry is denied and security forces are alerted.

The intelligent building

Depending on the level of security required to protect the facility and the information stored within, the intelligent building has two functions — keeping unauthorized personnel out, and assisting authorized personnel with their daily responsibilities and, for the most secure facilities, tracking and recording all activities while in the building. In our scenario, the next layer of access control is at the building entrance. Once again, the ever-watchful surveillance cameras continuously scan the entryway for

activity. When someone enters the field of view, it alerts the security team and attempts to identify the person. It determines if more than one person is present. As a visitor approaches the door, they present their token (smart card or other device) to a reader. Or they present their biometric identity (fingerprint, iris, face, etc.) to a reader. The door opens if their identity has been verified and entry is authorized. If not authorized, the individual is denied entry or trapped in a mantrap until security personnel arrive.

Let’s assume I am the person at the door and I am granted access. The computer now knows I’m in the building. As I go through the various access points passing through a variety of biometric screens and access control devices on the way to my office, the computer is kept up-to-date of my location and my activities. Doing something that is not in my daily routine, like attempting to enter an unauthorized area or avoiding one of the checkpoints, trips an alarm. If I’m scheduled to be on vacation and an attempt is made to log in to my system by someone, security is immediately notified.

The avatar and the intelligent office

As I approach my office, a camera on the door — or a fingerprint recognition pad, whatever kind of biometric is chosen — controls access. Upon positive identification, the door opens and my electronic assistant, an avatar — an animated stand-in graphic — greets me and begins bringing up my workstation. Sensitive computing technology is used to equip me with the tools I need to be more efficient in my work. The computer has turned on my lights, opened my blinds, unlocked the storage cabinets that I may need to access, turned on my computer and logged me into the system. The screen is still locked, but it’s on. As I sit down at my computer, another camera on top of the computer recognizes me and automatically unlocks my screen. Similarly, when I get up, the system automatically locks my screen again. The software applications and network access are all controlled by biometrics. These are face, fingerprint, iris, or voice-enabled. When I go into an application that our security policy has restricted — a different biometric identity authorization is requested.

I know where you've been

Let's say I attempt to get into an application, or a database that I have never used without authorization. The intelligent office detects that I'm doing something I don't normally do. It queries if I'm sure that I want to go into this, and alerts security that I'm doing something out of the ordinary. Why is this important? If someone has managed to get through the fence, stolen my identity and is attempting to use my computer — security needs to be alerted. If I am at the keyboard, then I will be held accountable. With sensors installed throughout the facility, the intelligent office tracks the activities and locations of all personnel. If any event comes up in the future that requires investigation, the system can recall exactly what the suspect did that day.

Guest or perpetrator?

If I have a guest when I attempt to enter the intelligent building or office, the surveillance camera recognizes me and sees there's someone very close. The system is also intelligent enough to know that the person with me could be a friendly visitor or a potential terrorist. It checks my profile to see if I'm authorized to be an escort. If so, it looks at us and analyzes our behavior characteristics for signs of duress — and allows or denies entry, alerting security either way.

When the building allows us to enter, an "Unknown Visitor" icon immediately appears on the office personnel location board and on everyone's screen in the facility alerting all that an unidentified visitor is on premises. Once I escort my visitor to the enrollment station, where their personal information and biometrics are captured and stored in the database, the icon on everyone's screen is replaced with the photo of the individual and their name — color-coded with classified/non-classified access. This identifies whether or not we can discuss any classified information while that individual is in the facility. This stays up until the visitor departs the facility. While in the high security area, all activities are recorded. Upon leaving, the board is cleared and the information on their activities stored.

Fantasy or reality?

Think the above scenario is closer to a James Bond scene than real life? Think again. Federal officials told Congress on 25 April 2002 that they support the idea of using a combination of commercially available biometric technology and smart cards to identify every employee entering a federal building.¹ Most of the solutions discussed here are being used today to defend our homeland and critical infrastructure. While the intelligent building may sound futuristic, the basic tools and the technology are available today.

¹ "Smart building IDs gaining support, passes could include fingerprint scans," Judi Hasson, 29 April 2002, FCW.com

For more information, please visit our website at:
www.unisys.com

Specifications are subject to change without notice.

© 2008 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

Printed in the United States of America CMS 252-08 10/08



68707629-100