



Journal of Innovation

FOCUSING ON THE FUTURE OF TECHNOLOGY SPRING | SUMMER 2004

Grid Computing

Common Criteria:
Understanding the Mandate

Mars Exploration Rover:
Independent Verification
and Validation



BIOMETRICS:

Trust, But Identify

BY | John D. Woodward, Jr.
Director, U.S. Department of Defense
Biometrics Management Office

(This article is based on remarks Mr. Woodward made to the WHITC Foundation earlier this year)

The Department of Defense (DoD) has a growing need to control access to its many assets in both times of war and peace. Similarly, DoD organizations must always be ready to identify "friend or foe." This requirement is heightened in the Global War on Terrorism, where the enemy has demonstrated its willingness to exploit flaws in current identity management systems. Identity assurance is vital to protecting our facilities, our information networks and, most important of all, our personnel. Biometric systems take identity assurance beyond something you have (e.g., an identification card) or something you know (e.g., a password) to something you are (e.g., a fingerprint). The DoD, along with many other agencies, is looking at biometrics as a way to safeguard its assets. The DoD Biometrics Management Office, located in Arlington, Va., supports and encourages the use of biometric technologies in the Department. The Biometrics Fusion Center in Bridgeport, WVa., a subordinate unit of the Biometrics Management Office, provides testing and other operational support.

As Director of the Biometrics Management Office, I understand both the tremendous potential and the current realities of these technologies. Working together with Sam Cava, the Director of the Biometrics Fusion Center, I am committed to having DoD use biometric technologies effectively and efficiently, particularly to support the U.S. military's efforts in the Global War on Terrorism. In this article, I provide an overview of where we are today in building better biometric capabilities within DoD.

To provide that overview, this article:

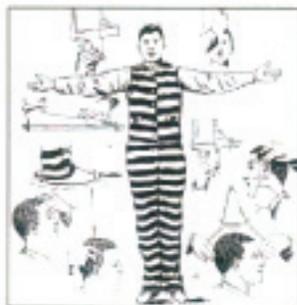
- » offers a brief historical perspective of biometrics;
- » defines the current situation and offers some examples of how currently available biometric technologies may or may not meet national security requirements; and
- » suggests an operational framework for examining how DoD can deploy biometric technologies.

Biometrics: A Historical Perspective

For most of the 19th century, when a person was convicted of a crime, the sentence was based on the specific offense

were not incentivized to disclose their past bad acts. To get to the truth, criminal investigators of the 19th century considered several potential solutions for linking a person's identity to that person's prior criminal record.

Initially, officers of the law tried to recognize previous criminals, primarily by their facial characteristics. This method worked well enough when the repeat offender was a member of a small community where he was well known. However, the system began to unravel as communities expanded and as populations became more mobile. Even with those factors removed, the truth is



committed. Other factors, such as the person's prior criminal history, had very little effect on the punishment a criminal received. With the passage of the Habitual Criminals Act in 1869, the British Parliament introduced a new criminal justice concept with punishment tailored not only to the specific offense committed, but also to a person's history of bad acts or prior criminal record. In other words, habitual criminals (or recidivists) received harsher sentences. This approach is still with us today and embodies society's views of criminal justice.

To comply with the new law, a person's history of criminal activity had to be matched to his or her identity, particularly since persons with prior criminal records

that most people - even trained police officers - are not very good at recognizing faces of people they do not know well. Thus, innovators searched for technology that could aid in identification.

Alphonse Bertillon, a Paris police official, came to the apparent rescue with anthropometrics, which involved taking multiple measurements of an individual, such as the length of the arm from the elbow to the tip of the index finger, using specially designed tools and recording the information on a record card (see illustrations).

The general premise was that a trained law enforcement officer could use these unique physical characteristics to

distinguish an individual from all others in a population. The police would take anthropometric measurements of a person and compare all the record cards for matches. This "Bertillonage" was an early attempt by the criminal justice community to use biometrics to determine identity.

In 1884, Bertillon made 200 matches of persons with prior criminal records that the police had otherwise missed. In the end, anthropometrics did not prove to be the silver bullet that the police had hoped. There were discrepancies in measurements taken by different people, the "enrollment" was overly complex and

Investigation (FBI), astutely and skillfully recognized how fingerprints would be useful for identification purposes and established the FBI as the steward for criminal fingerprint data in the U.S. That legacy eventually led to the creation of the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Launched in 1999, IAFIS is the FBI's computer-searchable database, located at the Criminal Justice Information Services Division in Clarksburg, W. Va. IAFIS basically contains the fingerprints of about 46 million individuals who have been arrested for felony-level offenses in the United States. Today, one of the first steps

history consumer information and general biographical data such as name, address and phone number.

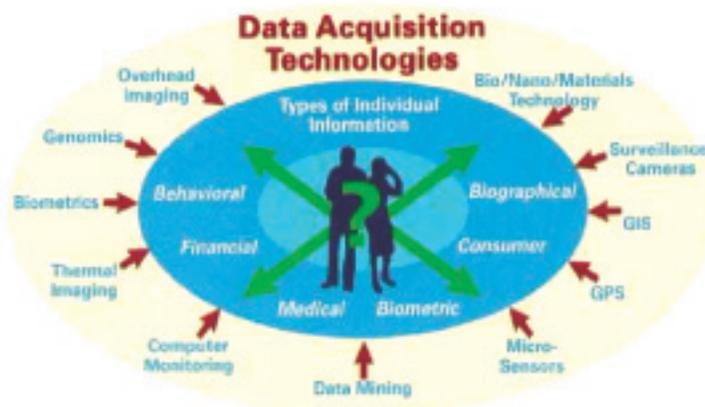
The question is: How can we best obtain and make sense of the individual information in one or more of these categories? Various Data Acquisition Technologies (DATs) have emerged to capture and collect individual information. They are referenced in the outermost circle of the illustration and include tools like the Global Positioning System (GPS), thermal imaging, overhead imaging or satellite reconnaissance, as well as various forms of data mining and computer monitoring.

Biometrics is another example of a DAT. As such, biometrics can help link a present individual to previously used identities and past acts, and perhaps even link a present individual to anticipated future acts.

This places us in a position not unlike that of the 19th century: Then as now, legal and policy decisions have created operational requirements for which we need technology solutions. The technical, operational and administrative parameters of that time led to the eventual adoption of fingerprinting, a solution that is still valid and widely used today. In seeking biometric solutions to newly emerging requirements - especially in the force protection, national security and counterterrorism arenas - it is critical to identify not only the requirements themselves, but also the technical, operational and administrative needs that will lead to successful implementation of technologies.

National Security Needs and Biometric Realities

To establish and verify identity in everyday transactions, we have gone from what we have, such as tokens, badges and keys, to what we know, such as PINs, pass codes, passwords and secret phrases. Now we are moving from what we know to what we are, which entails the linking of identity to



time-consuming, and anthropometrics are not left behind at crime scenes.

Fortunately, at about the same time, there was a competing school of thought in criminal justice that advocated the use of fingerprints - another form of biometrics - as a means of determining identity. Publicized in 1878 by Dr. Henry Faulds, a British missionary working in Japan, this approach relied on the distinctive patterns on a person's fingers to ascertain identity. In 1902, fingerprints were used for the first time in an English court of law to convict someone of a crime. In the United States, fingerprints were used for the first time in a courtroom in 1911 to determine guilt.

In the 1920s, J. Edgar Hoover, the young director of the U.S. Federal Bureau of

Investigation (FBI), astutely and skillfully recognized how fingerprints would be useful for identification purposes and established the FBI as the steward for criminal fingerprint data in the U.S. That legacy eventually led to the creation of the FBI's Integrated Automated Fingerprint Identification System (IAFIS). Launched in 1999, IAFIS is the FBI's computer-searchable database, located at the Criminal Justice Information Services Division in Clarksburg, W. Va. IAFIS basically contains the fingerprints of about 46 million individuals who have been arrested for felony-level offenses in the United States. Today, one of the first steps

Where is Biometrics Today?

Where do biometrics fit into the current picture? The above illustration helps explain.

Individual information, shown in the inner circle, consists of many types. These include biometric data, medical information, financial information, credit

CONTINUED ON PAGE 22

physical characteristics or personal traits.

Three of the most commonly cited reasons for using biometrics are:

1. to provide better security;
2. to increase convenience; and
3. to save money or provide a return on investment.

These benefits have yet to be proven by hard, empirical data and many times require case-by-case analysis. A requirement the U.S. has right now has the potential to help make the case for use of biometrics. It is the fundamental need to vet and fix a person's identity. The requirement is nothing new. What is new is the context.

Today, it is possible for an individual who has been dismissed from a job with the DoD to gain employment in another position at another DoD installation. All he or she needs is a new alias name and easily obtainable fraudulent identity documents to support that alias name. Biometrics could help resolve this problem by permanently linking a person with his or her identity.

The homeland security arena offers another new-context requirement to vet and fix identity. The U.S. Departments of Homeland Security, State and Justice are all working together to prohibit potentially harmful persons from entering the United States. Again, a major question is how best to stop an individual with a criminal or terrorist record from obtaining a U.S. entry visa from a U.S. embassy abroad when that person is using a new alias and forged documents. As things currently stand, it is difficult to make the link between the person claiming to be *x* when he or she is really *y*. Biometric technology solutions are now being employed to help thwart this problem.

Not only do these examples define a requirement to vet and fix identity, they do so in new contexts with new technical, operational and administrative parameters.

Which of the various biometric technology solutions, if any, is going to be

effective in addressing the requirement? That is what we are attempting to determine in the DoD.

First, the DoD has to consider the technical limitations of current biometric systems, particularly in looking at enterprise-wide solutions. Second, with three separate Service departments and a large number of support agencies and offices, the DoD must consider a wide range of operational and procedural issues

There are three parts to this framework - Foundation, Applications and Drivers. Identity Authentication, or the vetting and fixing identity, is at the Foundation level. This gets to the one-individual/one-identity objective.

The Applications level considers how the data available in the Foundation level is used. Logical access and physical access applications address the question of verification, using biometrics as a way to



in searching for ideal verification and identification solutions. For example, the Biometrics Management Office stresses interoperability of biometric technologies throughout DoD. Third, there are legal, policy and social concerns, especially in the privacy arena. In sum, these considerations - technical, operational, procedural, legal, policy and social - constitute the practical parameters that determine whether, to what degree, and/or how we can use biometrics within the Department of Defense to address security requirements.

An Operational Framework for Approaching Biometrics

The Biometrics Management Office has developed a basic operational framework (see illustration) as a means to better understand the DoD's requirements as well as the technical, operational, procedural, legal, policy and social parameters in which we work.

ensure that only authorized persons are able to access DoD locations, computers, information and networks.

Accountability entails the application of biometrics to monitor and record activities and movement and to prevent fraud and abuse.

The Drivers level refers to the reasons that the DoD might have for actually using the biometric data that it has or may eventually obtain. These reasons include national security concerns as well as the need to improve business processes and optimize resources. By using this framework, we are better able to identify, understand and intelligently apply biometric technology solutions within specific DoD contexts.

Summary

In essence, biometrics is a high-tech word for an old concept, human recognition. Just as the 19th century criminal justice system developed a requirement to link a

person to his previously used names and past activities, so, too, the DoD is developing requirements in force protection, national security, and counterterrorism areas that biometric technologies can help support. Today, biometrics help protect the integrity of vital U.S. Government information and installations around the world.

The Biometrics Management Office, and its operational arm, the Biometrics Fusion Center, are leading efforts to encourage the use of biometric technologies throughout DoD. We are actively working with many U.S. Government agencies, including the FBI's Criminal Justice Information Services Division, to leverage resources and ensure interoperability for the effective deployment of biometrics throughout the DoD, particularly in support of the Global War on Terrorism. The staffs of the Biometrics Management Office and Biometrics Fusion Center are proud to serve the national security community in this effort.

(The views and conclusions expressed in this presentation are those of Mr Woodward and do not necessarily represent those of the U.S. Department of Defense or any of its components, the RAND Corporation or any of RAND's research sponsors.)

Mr. Woodward comes to the Department of Defense Biometrics Management Office from RAND Corporation under the authority of the Intergovernmental Personnel Act, which permits movement of personnel between qualifying organizations. At RAND, he served as a senior policy analyst working on national security, intelligence and technology policy issues for various U.S. Government clients. Mr. Woodward's particular area of interest is biometrics. He has testified about biometrics before Congress, the Commission on Online Child Protection and the Virginia State Crime Commission. He is the primary author of *Biometrics*,

Identity Assurance in the Information Age (McGraw Hill, 2003). Prior to joining RAND full-time in 2000, Mr. Woodward served as an Operations Officer for the Central Intelligence Agency for 12 years. A member of the Virginia State Bar, Mr. Woodward received his Juris Doctor degree magna cum laude from Georgetown University Law Center in Washington, D.C. He was a Thouron Scholar at the London School of Economics, University of London, where he received his M.S. in Economics. He received his B.S. in Economics from the Wharton School of the University of Pennsylvania. Contact Information: john.woodward@hqda.armymil ♦

Editor's Note: In 2000, U.S. Senator Robert C. Byrd appropriated federal funds which led to the creation of the Biometrics Fusion Center positioning West Virginia on the cutting edge of biometrics technology.