September 2005

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

BIOMETRIC TECHNOLOGIES: HELPING TO PROTECT INFORMATION AND AUTOMATED TRANSACTIONS IN INFORMATION TECHNOLOGY SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Biometric technologies are crucial components of secure personal identification and verification systems, which control access to valuable information, to economic assets, and to parts of our national infrastructure. Biometric-based identification and verification systems support our information-based economy by enabling secure financial transactions and online sales, and by facilitating many law enforcement, health, and social service activities. Since September 11, 2001, our national requirements to strengthen homeland security have intensified, stimulating government and industry interest in applying biometric technologies to the automated verification of the identity of individuals.

What Are Biometrics

Biometric technologies are automated methods for identifying a person or verifying a person's identity based on the person's physiological or behavioral characteristics. Physiological characteristics include fingerprints, hand geometry, and facial, voice, iris, and retinal features; behavioral characteristics include the dynamics of signatures and keystrokes. Biometric technologies capture and process a person's unique characteristics, and then authenticate that person's identity based on comparison of the record of captured characteristics with a biometric sample presented by the person to be authenticated. After many years of research and development, biometric technologies have become reliable and cost-effective, and acceptable to users. New applications of biometrics are being successfully implemented in more secure travel documents, visas, and personal identity verification cards. These applications help to safeguard valuable assets and information, strengthen homeland security, and contribute to the safety and security of automated transactions.

Interest in Applications of Biometric Technology

Both public and private sectors are looking for reliable, accurate, and practical methods for the automated authentication of identity, and are using biometric technologies in a wide variety of applications, including health and social service programs, passport programs, driver licenses, electronic banking, investing, retail sales, and law enforcement.

Authentication systems are usually characterized by three factors:

- Something that you know, such as a password,
- Something that you have, such as an ID badge, and/or
- Something that you are, such as your fingerprints or your face.

Systems that incorporate all three factors are stronger than those that use only one or two factors. Authentication using biometric factors can help to reduce identity theft and the need to remember passwords or to carry documents, which can be counterfeited. When biometric factors are used with one or two other factors, it is possible to achieve new and highly secure identity applications.

Continued on Page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community.

Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since June 2004:

- *Information Technology Security Services: How to Select, Implement, and Manage*, June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance for Selecting Secure Techniques*, August 2004
- *Information Security Within the System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA, November 2004*
- *Integrating IT Security into the Capital Planning and Investment Control Process, January 2005*
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* April 2005
- *Recommended Security Controls for Federal Information systems: Guidance of Selecting Cost-effective Controls Using a Risk-based Process, May 2005*
- *NIST's Security Configuration Checklists Program for IT Products,* June 2005
- *Implementation of FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2005*

For example, a biometric factor can be stored on a physical device, such as a smart card that is used to verify the identification of an individual. Today, the identification cards that are issued to employees for access to buildings and to information, and the cards that are used for financial transactions, often include biometric information.

Biometric factors can also be used with encryption keys and digital signatures to enhance secure authentication. For example, biometric information could use public key infrastructure (PKI) systems that incorporate encryption (such as Federal Information Processing Standard [FIPS] 197, *Advanced Encryption Standard*). Encrypting the biometric information helps to make the system more tamper resistant.

NIST Role in Biometrics

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) has been a major contributor to the development of measurements, standards, and tests for biometrics for many years. Areas of investigation include fingerprints, face recognition, iris recognition, and speech recognition. NIST supports the development of voluntary industry standards and the development of conformance tests, reference implementations, and evaluation procedures to facilitate the implementation of standards in biometric products. Recent legislation directed NIST to work with other federal agencies to develop standards needed for the biometric authentication of applicants for U.S. visas. In advancing the development of measurements and standards for biometrics, NIST works in close cooperation with industry, national and international standards groups, and federal, state, and local government organizations.

This bulletin summarizes some of NIST's activities to support biometric standards and measurements, and updates the ITL Bulletin issued in May 2001 detailing NIST's biometric technology and standards activities: *Biometrics – Technologies for Highly Secure Personal Authentication*, by Fernando L. Podio. Information about NIST, industry, and standards activities, as well as listings of publications and references, is available on the Biometrics Resource Center website:

http://www.nist.gov/biometrics

Under the Federal Information Security Management Act of 2002 (FISMA), NIST develops standards and guidelines to protect the security and privacy of sensitive unclassified information processed in federal computers. NIST supports the development of voluntary industry standards, both nationally and internationally, as the preferred source of standards to be used by the federal government, enabling it to rely upon the private sector to supply it with goods and services (National Technology Transfer and Advancement Act of 1995 [Public Law 104-113]). NIST's Information Technology Laboratory (ITL) has been accredited as a standards developer by the American National Standards Institute (ANSI).

Information about ITL's information security activities is available from the Computer Security Resource Center at:

http://csrc.nist.gov/

New Requirements for Homeland Security

The need for tests, measurements, reference data, and other technical tools to support the development of biometric technologies became more critical with threats to U.S. homeland security. The USA PATRIOT Act (Public Law 107-56) provides that other federal organizations work with NIST to "develop and certify a technology standard that can be used to verify the identity of persons applying for a United States visa . . ." The Enhanced Border Security Act (Public Law 107-71) spells out requirements for reviews of the effectiveness of biometric technology currently in use, and supports the development of new biometric technology for identification verification. Public Law 107-173, the Enhanced Border Security and Visa Entry Reform Act of 2002, established requirements for the development of a technology standard based on biometrics to verify the identity of persons applying for visas to the United States. Homeland Security Presidential Directive (HSPD) 12, issued in August 2004, called for the development of a mandatory, governmentwide standard for secure and reliable forms of identification for government employees and contractors.

NIST Studies and Investigations

NIST scientists and engineers have a great deal of experience in using computers to match images automatically. There have been long-standing efforts to assist the law enforcement community in developing and improving automated methods for fingerprint matching, in evaluating facial recognition systems, and in acquiring information systems that support the Department of Justice's Automated Fingerprint Identification System (AFIS). Much work has been done to develop test data for use in evaluating automated optical character recognition (OCR), fingerprint classification and matching, and face recognition systems. The test data help both users and implementers of recognition systems in evaluating the effectiveness of these systems. A listing of publications and test data collections related to NIST's past and ongoing investigations and studies on the automated recognition of fingerprints, faces, and handwritten characters is available at:

http://www.itl.nist.gov/iaui/894.03/pubs.html#fing

In response to the USA PATRIOT Act and the Enhanced Border Security Act, NIST studied biometric technologies to evaluate their potential for enhancing border security. These evaluations examined applications that would positively identify visa applicants and verify that the holder of a visa is the person to whom the visa

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or Elizabeth.lennon@nist.gov

was issued. Fingerprint performance was measured on an Immigration and Naturalization Service (INS) database of 1.2 million prints of 620,000 individuals. Face Recognition Vendor Tests (FRVT) carried out in 2002 measured face recognition performance of ten vendors on a Department of State database of 121,000 images of 37,000 individuals. Based on the evaluations, as well as practical considerations about the amount of data that can be stored on a smart card, NIST recommended that at least two fingerprints be used to positively identify visa applicants and that a dual system of face and fingerprint recognition be used to verify the identities of visa holders at points of entry into the United States. The FRVT 2002 was supported by the Defense Advanced Research Projects Agency (DARPA), the Departments of Defense, Justice and State, and other federal agencies.

A Fingerprint Vendor Technology Evaluation (FpVTE) conducted in 2003 evaluated the accuracy of fingerprint matching, identification, and verification systems. This evaluation was conducted by NIST on behalf of the Justice Management Division (JMD) of the U.S. Department of Justice to assess the capability of fingerprint systems in meeting the requirements for law enforcement matching systems, visitor and immigrant status programs, and implementer software development efforts. Multiple tests were performed with combinations of fingerprint data, such as single fingers, two index fingers, four to ten fingers, and with different types and qualities of operational fingerprints, such as flat live-scan images from visa applicants, multi-finger slap live-scan images from booking or background check systems, or rolled and flat inked fingerprints from law enforcement databases.

The most accurate systems were found to have consistently low error rates across a variety of data sets. System accuracy was improved when four or more fingerprint images were used. The tests also showed that the most accurate fingerprint systems are more accurate than the most accurate facial recognition systems. Results are expected to form the basis for the design and acquisition of large-scale fingerprint identification systems, such as for entry and exit systems to the United States.

More information about the evaluations is available at:

http://www.frvt.org

Biometric technologies are essential to the implementation of Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, which was developed in accordance with the requirements of HSPD 12 and approved in February 2005 by the Secretary of Commerce. FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that supply PIV cards as identification credentials and that use the cards to authenticate an individual's identity. Draft NIST Special Publication (SP) 800-76, *Biometric Data Specification for Personal Identity Verification*, by Charles Wilson, Patrick Grother, and Ramaswamy Chandramouli, was developed to provide the technical specifications for the biometric data specified in FIPS 201. The publication details the technical requirements for capturing and formatting fingerprint and facial image information to be included on PIV cards. The technical requirements are based on voluntary industry standards, providing guidance for implementers when there are options in the standards that would interfere with interoperability if the options were to be implemented in different ways.

Information about FIPS 201 and the PIV program at NIST is available at:

http://csrc.nist.gov/piv-program/index.html

Biometric Consortium

The U.S. Biometric Consortium (BC), which has been meeting since 1995, includes more than 900 representatives from federal, state, and local governments, academia, and industry, who work together to coordinate and advance the development of biometric technologies. Over half of the participants in the consortium are from industry, and more than 60 federal agencies, including the executive departments and the military services, participate. The BC sponsors technology workshops, standards activities, and user activities to address research and technology evaluation efforts. The BC's annual conference, which is open to members and the general public, is now the largest biometric conference in the world.

NIST and the National Security Agency (NSA) co-chair the Biometric Consortium. Information about BC activities is available on the website:

http://www.itl.nist.gov/div893/biometrics/consortium.html

Common Biometric Exchange Formats Framework (CBEFF)

In 1999, the Biometric Consortium initiated the development of a common data format to facilitate the exchange and interoperability of biometric data. Industry and government representatives identified the need for a technology-blind biometric format that would facilitate the handling of different biometric types, versions, and biometric data structures in a common way. This common format would facilitate the exchange and interoperability of biometric data for all aspects of biometrics, independent of the particular vendor that generates the biometric data. The initial conceptual definition was achieved through a series of workshops co-sponsored by NIST and the Biometric Consortium. A technical development team led by NIST and NSA developed the Common Biometric Exchange File Format. It was published by NIST as NISTIR 6529, *Common Biometrics Exchange File Format (CBEFF)*, in January 2001. An augmented and revised

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

version of the CBEFF was issued as NISTIR 6529A, *Common Biometric Exchange Formats Framework*, in April 2004.

The CBEFF describes a set of data elements necessary to support biometric technologies in a common way independently of the application and the domain of use, such as mobile devices, smart cards, protection of digital data, and biometric data storage. CBEFF facilitates biometric data interchange between different system components or between systems. It promotes interoperability of biometric-based application programs and systems, provides forward compatibility for technology improvements, and simplifies the software and hardware integration process. The CBEFF was augmented by the NIST/BC Biometric Interoperability, Performance and Assurance Working Group to incorporate a compliant smart card format, product identification (ID), and a CBEFF nested structure definition. The augmented CBEFF was submitted to the INCITS M1 committee for processing as a national standard and has been published as American National Standard INCITS 398-2005. The international version of CBEFF is in the last stages of development and is expected to become an ISO standard at the end of 2005.

NISTIR 6529A is available at:

http://www.itl.nist.gov/div893/biometrics/documents/NISTIR6529A.pdf

Other Organizations Supporting Biometric Technology

The **National Biometric Security Project** (NBSP) is an independent not-for-profit corporation, which supports non-defense government and private sector efforts to protect the security of the civil infrastructure from terrorist threats through the application of proven biometric technologies. More information is available at:

http://www.nationalbiometric.org/nbsp.html

The Department of Defense (DoD) **Biometrics Management Office** (BMO) is responsible for leading, consolidating, and coordinating the development, adoption, and use of biometric technologies for the Department of Defense to support the warfighter and enhance Joint Service interoperability. More information is available at:

http://www.biometrics.dod.mil/

The **BioAPI Consortium** was founded to develop a biometric Application Programming Interface (API) to allow for platform and device independence to application programmers and biometric service providers. The BioAPI Consortium is a group of over 120 companies and organizations that have a common interest in promoting the growth of the biometrics market. The BioAPI Consortium developed a specification and reference implementation for a standardized API that is compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies. More information is available at:

http://www.bioapi.org/

The **Biometric Interoperability, Performance and Assurance Working Group** was established by NIST and the Biometric Consortium to broaden the utilization and acceptance of biometric technologies and to facilitate and encourage further exchange of information and collaborative efforts for biometrics between users and private industry. The Working Group (WG) supports the advancement of technically efficient and compatible biometrics technology solutions on a national and international basis. The WG addresses issues and efforts other than those efforts already under way in national or international organizations, such as formal standards bodies, industrial consortiums, and cooperative testing activities. In addition to developing the Common Biometric Exchange Formats Framework (the augmented and revised version of CBEFF), the WG developed a specification defining methods for biometric template protection and a biometric Application Programming Interface for Java Card.

Support for Voluntary Standards Development

NIST has contributed to the development of national and international standards for biometrics. These standards are considered to be critical for U.S. needs for homeland security, the prevention of identity theft, and for other government and commercial applications based on biometric personal authentication. These standards are essential for achieving the connectivity and interoperability of different systems and for assuring security. As an accredited standards developer, NIST/ITL has sponsored the development of voluntary industry standards for the interchange of fingerprints, facial data, and scar, mark and tattoo (SMT) data.

For the past seven years and particularly since September 11, 2001, NIST has intensified its work in support of the development of biometric standards by working with consortia and other industry groups. NIST strongly backs national and international standards organizations as the best environments for the development of voluntary consensus standards for biometric technology and the deployment of standards-based solutions. Priorities for homeland security have been driving efforts to develop high performance interoperability standards for biometrics. Interest in standards for smart cards has also intensified.

The chief U.S. venues for these standardization efforts are the InterNational Committee for Information Technology Standards (INCITS) Technical Committees M1, for biometrics, and B10, for smart cards. In addition to developing national standards, the M1 and B10 committees act as the U.S. technical advisory groups (TAGs) to subcommittees in International Standards Organization/ International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 (JTC 1). INCITS M1 is the TAG to ISO/IEC JTC 1 Subcommittee 37 – Biometrics. INCITS B10 is the TAG to ISO/IEC JTC 1 SC 17 - Cards & Personal Identification.

NIST contributes to the work of INCITS M1 and to JTC 1 SC 37 by providing leadership, including committee officers, technical editors, and other technical

expertise. The committees' work includes the development of standards and specifications for biometric data formats for finger, facial, iris, and signature recognition; the development of application profiles for transportation workers, border crossing, and point-of-sale; and biometric performance evaluation and reporting methods. Since its first meeting in January 2002, the INCITS M1 committee has developed many needed biometric data interchange and interoperability standards, which have been approved as American National Standards Institute (ANSI) standards: seven biometric data interchange standards and two biometric application profiles. Two biometric interface standards (the BioAPI specification and the Common Biometric Exchange Framework Format) were also approved by INCITS. In 2005 ISO approved and published four biometric data interchange standards that had been developed by JTC 1 SC 37. In the United States, large government organizations are adopting many of the INCITS biometric standards that have been approved as American National Standards. Large international organizations are adopting the international standards emerging from JTC 1 SC 37. Other standards that will contribute to the successful deployment of secure, interoperable, reliable, and cost-effective information systems are currently under development in these national and international standards groups.

Voluntary industry standards to which NIST has made significant contributions include:

- X9.84-2000, *Biometrics Management and Security for the Financial Services Industry*. This standard specifies the minimum security requirements for effective management of biometrics data for the financial services industry and security for the collection, distribution, and processing of biometrics data.

- ANSI/NIST-ITL 1-2000, *Data Format for the Interchange of Fingerprint, Facial, and Scar, Mark and Tattoo (SMT) Information*. This standard revises and consolidates earlier standards developed by NIST to specify a common format for exchanging biometric data across jurisdictional lines or between dissimilar systems made by different manufacturers. Originally published as NIST Special Publication 500-245, the specifications were advanced to the status of national standards in accordance with ANSI procedures for the development of standards using the canvass method.

Conformance Testing in Support of Users and Product Developers

Standards-based, high-quality conformance testing helps both developers and users by validating conformance claims, leading to greatly increased levels of confidence in products. Testing can also help to ensure interoperability between standards-based products and systems. NIST and the Department of Defense (DoD) Biometrics Management Office (BMO) have been working in close collaboration in the development of biometric standards and supporting testing tools. For more than a year, NIST and the BMO have been independently developing implementations of BioAPI test tools. These test tools will support users within DoD and other government agencies already requiring, or intending to require in the near future, that Biometric Service Providers (BSPs) conform to the BioAPI standard. The test tools will enable the future establishment of conformity assessment programs to validate conformance to the BioAPI standard and other emerging standards, and will help product developers interested in developing products conforming to voluntary consensus biometric standards to use the same test tools available to users.

NIST and the BMO are conducting intensive testing of the initial versions of the test tools to cross-validate the test results using a number of vendor BSPs that claim their products conform to the BioAPI standard. The initial test tool implementations were developed using concepts and principles specified in a draft conformance testing methodology standard that is currently under development in INCITS M1 committee. This documentary standard project was sponsored by NIST, the DoD BMO, the National Biometric Security Project (NBSP), Saflink Corp., and The Biometric Foundation (TBF). The NIST test tool implementation development was co-sponsored by the National Biometric Security Project. The principal developer is Saflink Corp.

Conclusion

After many years of involvement in biometric activities, NIST continues to investigate promising technologies and to advance the development of industry standards for biometrics. Although they are quite promising, biometric technologies are not the sole solution for controlling access to information or for verifying the identity of an individual. All biometric data must be protected appropriately, and biometric controls must be selected and used within an integrated security program that assesses risks to information and information systems, determines security requirements, and selects cost-effective management, operational, and technical controls.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900