Innovations in Biometric Authentication Technologies

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Examples of biometric technologies include fingerprint, face, speaker, iris, and hand geometry recognition. Biometric technologies are becoming the foundation for an extensive array of highly secure identification and personal authentication solutions.   Enterprise-wide network security infrastructures, Government IDs, secure electronic banking, investing and financial transactions, retail, law enforcement, and health and social services are already benefiting from these technologies.

With the advent of the new century, it has become apparent that there is a great need for biometrics. Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives...The need for biometrics can be found in commerce, in Federal, State and Local governments, in the military and in commercial applications. Trustworthy electronic commerce and electronic government, for example, can be achieved through the utilization of strong personal authentication procedures. Trust in these electronic transactions will be essential to the healthy growth of the global economy.

Who Should Attend:

This panel session will be of interest to anyone who would like to learn how biometrics are being used to address access control issues, particularly for workstations and enterprise systems. System security administrators, security product developers, enterprise managers, and others will benefit.

State-of-the-Art in Biometric Technologies (Jeff Dunn, Co-Chair Biometric Consortium)
- Examples of biometric technologies
- Potential application of biometrics for both logical and physical access control
- Government and industry interest in biometric technologies

Biometrics for Enterprise Solutions (Cathy Tilton, Director for Enterprise Solutions, SAFLINK)
- Issues in applying biometrics for enterprise security
- Biometrics in a client / server environment
- Adoption of BioAPI interface specification

Emergence of Biometric Standards (Fernando Podio, Co-Chair Biometric Consortium)
- Common Biometric File Format Exchange specification
- Integration of biometrics and smart cards
- Activities in electronic commerce and other areas

Panelists

Jeff Dunn, Moderator (National Security Agency)
Co-Chair Biometric Consortium
Dunn@biometrics.org

Jeff Dunn is Chief of the Identification and Authentication Research Branch at the National Security Agency. This group is researching new technologies to protect access to computer systems in the Department of Defense and other critical systems. During his 20-year career at NSA, he has held a variety of program manager and management positions. Mr. Dunn is Co-Chair of the Biometric Consortium. The Biometric Consortium has over 800 members from Government, Industry, and Academia and serves as a focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology. Mr. Dunn has provided consultations on biometric technologies to a wide range of Government organizations.

Fernando Podio (National Institute of Standards and Technology)
Co-Chair Biometric Consortium
Podio@biometrics.org

Fernando Podio has been involved in information technology development, measurements, and standards development efforts for many years. He is a member of the National Institute of Standards and Technology (NIST), Information Technology Laboratory. He is currently the Program Manager for NIST's Biometrics and Smart Cards Program. This program is conducting research into the interoperability and performance of biometric subsystems, devices and applications, and the integration of biometrics and smart cards. Mr. Podio serves on the BioAPI Consortium Steering Committee and chairs the BioAPI Consortium's External Liaisons Working Group

Cathy Tilton (Director, Enterprise Products, SAFLINK)
Chair, BioAPI Consortium Steering Committee
CaTilton@aol.com

Cathy Tilton was one of the original developers of the the Human Authentication – API, developed under sponsorship from the Department of Defense. She now chairs the Steering Committee for the BioAPI Consortium. The BioAPI Consortium, which merged HA-API and other efforts, was formed to develop a widely available and widely accepted API that will provide industry biometric solution developers, software developers, and system integrators an API that leverages existing standards to facilitate easy adoption and implementation. The BioAPI Consortium now has over 50 members.