Update on the US Government's Biometric Consortium

Joseph P. Campbell, Jr. and Lisa Alyea
{jpcampb, laalyea}@alpha.ncsc.mil
US Department of Defense, R2
Fort Meade, Maryland, USA
20755-6000

ABSTRACT

This talk is an update on the discussions of the Biometric Authentication Consortium held at previous CardTech/SecurTech conferences. The Consortium held its first meeting in October 1992 under the chairmanship of Dr. Benincasa. Since then, the Consortium has been meeting 2-3 times per year to provide a forum for information exchange on biometric-based personal identification/authentication technology among the Government, industry, and academia. In 1994, we broadened our scope by dropping Authentication from the name (to include identification) and Dr. Campbell and Ms. Alyea took over as chair and vice chair, respectively. The goals of the consortium remain largely the same under this new leadership. The current emphasis is on the formal approval of our charter and on the establishment of a national biometric test and evaluation laboratory.

MISSION & FUNCTION

The Biometric Consortium serves as a Government focal point for research, development, test, evaluation and application of biometric-based personal identification/authentication technology. The Consortium encourages the use and acceptance of biometric technology in areas of critical need, as well as concerning itself with maximizing performance, minimizing cost, and avoiding duplication of effort. The Consortium coordinates technological concerns and issues of performance and efficiency within the Government in order to serve the best interests of the taxpayer. To accomplish these objectives, the Consortium will:

- Promote the science and performance of biometrics
- Establish standardized testing databases, procedures and protocols
- Provide a forum for information exchange among the Government, industry, and academia
- Establish increased Government and commercial interaction
- Establish symposia/workshops to include the contributions of academia and private industry
- Establish a feedback mechanism for issues that are exposed during the actual application of this technology
- Address the safety, performance, legal and ethical issues surrounding this technology.

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 01121997	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Update on the US Government's Biometric Consortium	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Information Assurance Technology Analysis Center (IATAC) 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 5	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12/1/97	Report

4. TITLE AND SUBTITLE
Update on the US Government's Biometric Consortium

5. FUNDING NUMBERS

6. AUTHOR(S)
Joseph Campbell, Jr., Lisa Alyea

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This talk is an update on the discussions of the Biometric Authentication Consortium held at previous CardTech/SecurTech conferences. The Consortium held its first meeting in October 1992 under the chairmanship of Dr. Benincasa. Since then, the Consortium has been meeting 2-3 times per year to provide a forum for information exchange on biometric-based personal identification/authentication technology among the Government, industry, and academia. In 1994, we broadened our scope by dropping Authentication from the name (to include identification) and Dr. Campbell and Ms. Alyea took over as chair and vice chair, respectively. The goals of the consortium remain largely the same under this new leadership. The current emphasis is on the formal approval of our charter and on the establishment of a national biometric test and evaluation laboratory.

14. SUBJECT TERMS
Biometric Consortium, working groups, National Test Center

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

CHARTER

The DoD established a Biometric Consortium in 1992 as a direct source of information and advice and to serve as the focal point for coordinating and developing advanced biometric processing, testing, and evaluation techniques. The Consortium shall establish biometric recognition standardized test procedures to be used by US Government agencies and foster communications between them and establish a test facility. The Consortium serves as a Government focal point for research, development, test, evaluation and application of biometric-based personal identification/authentication technology. The Consortium is presently comprised of representatives from 6 departments of the US Government and the armed services. The Consortium plans to develop an independent assessment facility to evaluate and test evolving biometric devices. The DoD has invested funds to develop standardized testing procedures and methodologies. That work is progressing, but is not yet finalized. The Consortium will endorse and accept test procedures and then take steps to make them "national standards" or at least nationally accepted procedures. The Consortium is the US Government's primary source of technical information for biometric considerations. Its test, evaluation and advisory functions will contribute significantly to biometric systems development.

Membership

The Consortium is a technically oriented group. Membership in the Consortium is open to all US Government civilian and military departments, agencies, and their duly appointed representatives. The DoD provides the Chair.

Responsibilities

The Consortium promotes biometric research and the exchange of ideas and structures research to advance the state of the art. The Consortium will be a visible and influential body to deal with biometrics that will play an important role in network security, access control, verification, etc.

Functions

The Consortium shall pursue the following tasks over the next 5 years:

- Evaluate various biometric techniques (e.g., finger print, voice, and facial)
- Develop tests and evaluations for various biometric systems
- Evaluate various biometric systems
- Establish a national test facility
- Perform other functions as its members may assign.

WORKING GROUPS

The Consortium has a number of working groups geared toward specific problem areas and interests. The following subcommittees have been established:

The *Testing and Reporting Group* is responsible for establishing testing standards, developing performance testing protocols, defining a test facility, deciding upon the format for the reported results, providing a mechanism for the dissemination of final reports, and defining a

repository for reported information.

The *Vulnerability Group* has the same responsibilities as the Testing and Reporting Group, but viewed from the standpoint of internal or external vulnerabilities to biometric devices.

The *Database Group* is responsible for defining standards for each particular type of biometric database, collecting databases into one central location, and disseminating database information to Government entities who require it for testing purposes.

The *Ground Rules Committee* is responsible for disseminating information about the Consortium, promoting external relations and contacts, encouraging internal interaction, defining Consortium operating procedures, and addressing any legal or ethical issues that affect the Consortium.

The *Research and New Technologies Group* is responsible for keeping abreast of the latest research and innovations in the field of biometrics, as well as providing a repository for such information.

NATIONAL TEST CENTER

A key issue for our test and evaluation center is the development of test and evaluation method(s) for repeatable and statistically significant performance tests. That is, how can one obtain reliable receiver operating curves (ROC) from a device and make meaningful comparisons with ROCs of other, possibly nonbiometric (e.g., password), devices? We see 3 main kinds of tests that use humans, simulations, and recordings/reproductions.

If a human crew is used, how are they selected and calibrated? Will the same humans be needed for all future tests, or can a sufficiently large sample be used to make this unnecessary?

If simulations are used, what types of simulations will be used and how will they be used? If fabricated body parts are used, how shall they be constructed and used?

If recordings and reproductions are used, how will the sensor and recognition system be separated? In the voice world, speech can be recorded and played back into the device because the sensor and the verifier are usually separable. For multidimensional verifiers/identifiers (e.g., image-based systems), this is a difficult problem because some use adaptive scanning, etc., thus making the sensor and the verifier inseparable. Different devices might also require different illumination, poses, and resolution, thus complicating the recording of a database.

Real-world performance prediction is a complex problem, but should be of prime concern to the Center. For example, a device that measured 0.3% equal-error rate in a lab was found in the field to have a false-rejection rate of approximately 25% (at an unknown false-acceptance rate). It's conceivable, but doubtful, that this device's threshold was adjusted between the lab and field tests to allow almost no false acceptances.

How will reasonable prediction of real-world performance be accomplished? How will different "real-worlds" (e.g., an unattended and unsupported device in an uncontrolled environment vs a guarded and maintained device) be accounted for?

For example, to test the hypothesis that the actual false rejection (FR) rate is less than or equal to 1% at 75% confidence requires 8 or fewer errors in 1,080 independent tests (for a 70% probability of passing the

test if the ratio of the true system error rate to the target error rate is 2/3) [1]. These tests are based upon the independence assumptions used in the collection and proper use of the YOHO database, Poisson's approximation to the binomial, error rates less than 5%, and sample sizes greater than 100.

In addition to using the critical number of errors tests, a number of other reporting means are of interest [2]:

- Raw error rates (relative frequency)
- Histograms of the number of errors vs number of individuals for each error type (e.g., subject falsely rejected, subject falsely accepted as another, and another falsely accepted as subject)
- Receiver operating curves, preferably bracketed by error bars
- The **d´** measure (the difference between the standard normal scores of the false rejection and correct rejection rates)
- A histogram of the identification rank
- Average identification rank

Fine-grain results on problem individuals can be informative (e.g., 3-D plots of attacker's vs attackee's identification numbers vs number of false acceptance errors).

CONCLUSIONS

The Biometric Consortium is growing in strength and numbers. Our joint efforts will, hopefully, bring about a national test center. This test center will bring maturity, reliability, and repeatability to biometric testing that is nearly absent today.

FURTHER INFORMATION

The Consortium's primary means of communication is an Internet listserv. Information about the listserv may be obtained by sending e-mail to the authors. We also hope to have information available on the AfB Biometrics' World Wide Web homepage at the URL:

http://www.npl.co.uk/~dsg/afb.html

REFERENCES

[1] Higgins, A., L. Bahler, and J. Porter. "Speaker Verification Using Randomized Phrase Prompting." *Digital Signal Processing* 1, no. 2 (1991): 89 - 106.

[2] Campbell, J. P., Jr. "Testing with the YOHO CD-ROM Voice Verification Corpus." To appear in *International Conference on Acoustics, Speech, and Signal Processing in Detroit,* IEEE, 1995.

Dr. Joe Campbell