

## **Continuous Identity Authentication Using Multi-modal Physiological Sensors**

The research proposed is for the construction and evaluation of an automated biometric system using a set of different unobtrusive physiological sensors (i.e., eye tracking & biosensors) that continuously authenticate the identity of the user. The system is designed to provide an added layer of security beyond point-of-entry identification methods and can be used in high and moderate security applications.

### **Problem Description**

Unauthorized access is a major security problem that yearly causes millions of dollars of damage, causes millions of person-hours to correct, causes injuries and in critical cases can cost lives. Authenticating the identity of an authorized user for access to a location or for use of a vehicle or device can be done in three different ways. The first method is by the use of something a person carries, such as a token, key or smart card. The second method is by the use of something a person knows, such as a password or personal identification code. The third method is by the use of a person's unique physical or behavioral attributes. Most access security systems use one or more methods to authenticate the user's identity, with the emphasis in biometrics on high accuracy point-of-entry identification devices such as a fingerprint or an iris scanner.

For location access, such as to a building or a room, a high accuracy point-of-entry identification maybe sufficient, but with vehicle or computer access, how would you know who's using these devices after initial access is authorized? For a higher level of security, continuous identity authentication especially for vehicle or computer access may be warranted.

An example of continuous authentication is a guard constantly watching over who is using a computer, using facial features and body movements as the biometric identifying attribute. Continuous identity authentication can prevent an unauthorized person from slipping in and using the computer system after the initial authentication of the identity of the authorized user.

Currently, our laboratory is doing research on an automated biometric system using a set of different physiological sensors (i.e., eye tracking & biosensors) that take passive measures of a user to continuously authenticate the identity of the user. The added layer of security continuous identity authentication provides beyond point-of-entry identification can be used in not only high security applications, but also in moderate security applications.

For example, in an emergency response situation, it is essential to be able to always "trust" all digital communication that provides information and manages resources. Otherwise, time is wasted since all digital communications must be challenged for authenticity. A biometric continuous identity authentication system can provide this additional layer of digital communication security.

The benefits of this systems over other biometrics is that multiple biosensors make the system difficult to defeat, passive sensors are more user acceptable and can be hidden, and a set of low cost biosensors that will produce nominal results can be used. Some applications include securing data entry, securing vehicle operation, securing firearms and securing computer operation. Applications for this system will be discussed in greater detail in subsequent sections of this proposal.

## **Introduction**

There are several types of biometric measures in current use. Biometric devices that measure fingerprints (e.g., U.S. Pat. No. 6,125,192), voice (e.g., U.S. Pat. No. 5,913,196), irises (e.g., U.S. Pat. No. 6,554,705), and facial images (e.g., U.S. Pat. No. 6,554,705) are available. All biometric devices require initial registration of the user's attribute that are measured by the sensors of the biometric device. Upon initial use to authenticate the identity of the user, current biometric devices extract a feature set from sensors which are correlated to an existing user database acquired during user registration. These devices require training, are time consuming, can be difficult to use, can require extra equipment, can be expensive and are so inconvenient that user identity authentication is done only upon initial use.

Other more unusual biometric devices include handheld writing devices that use writing pressure (e.g., U.S. Pat. No. 5,774,571 & 6,539,101), computer mouse index fingerprint (e.g., U.S. Pat. No. 5,991,431 & D440,568), body odor, ear shape and thermal imaging (Electronic Warfare Associates-Canada, Ltd., 2001).

These devices are designed primarily to provide authentication upon initial use and require training on the placement of the body part (e.g., finger). Another problem with many of the previously described biometric devices is that they rely primarily on the signal from a single sensor. A sensor flaw or signal distortion from that sensor could reduce the reliability of the user identity authentication system dramatically.

A multi-sensor biometric system would have many of one type of sensor (e.g., facial recognition cameras). The problem with this type of system is that if there is a general environmental factor that causes problems in one sensor, most likely all of the sensors will have the same problem. For example, poor lighting will reduce the efficacy of a multi-camera facial recognition system. A multi-modal sensor system would use several different modes of sensing biometric data. For example, sensing temperature, pulse rate & eye tracking, would be multimodal and less impacted by a single environmental problem.

For the past several years, we have been evaluating the potential of using data from physiological sensors to provide continuous identity authentication of a computer user. Below is a table of the physiological sensors we have been using and plan to use for continuous identity authentication.

Table 1. Physiological Measures

Physiological Measures	Secondary Measures	Equipment
Eye Position Tracking	Gaze Position, Fixation Number, Fixation Duration, Repeat Fixations, Search Patterns	ASL 501/504 or Alternate Eye Tracker
Pupil Size	Blink Rate, Blink Duration	
Skin Conductivity	Tonic and Phasic Changes	Custom Biosensor
Peripheral Temperature (Finger, Wrist & Ambient)		
Relative Blood Flow	Heart Rate and Beat to Beat Heart Flow Change	
Instrument Pressure Sensors	Grip Duration and Change	
Body Movement (planned)		

Individual patterns for many of the physiological measures being used could be used as biometric identifiers. Using passive multi-modal physiological sensors has the advantage of being unobtrusive, less vulnerable to single sensor errors and would be more difficult to circumvent than a single sensor system. When ready for real world use, this method could be inexpensively manufactured and require little or no training to use. Currently, we are researching methodologies to reliably extract salient biometrics for a continuous identity authentication system (CIAS).

Each of these physiological sensors produces data that has its own unique characteristics and methods for extracting secondary measures. For example, fixation number is determined from the tracked eye position. Variables involved in the definition of a fixation number includes the minimum amount of time spent looking at a single location and the definition of the size of that location. Changing either variable will change the number of fixations. These variables are defined by the experimenter and to be salient should be varied according to the nature of the task (e.g. reading text vs. searching for targets). This makes understanding the task being performed an important factor when using eye tracking data for identification and is likely true for all the other measures.

Some of the physiological measures do not provide useful biometrics information for a majority of people, but can be useful biometric identifiers for a significant number of people. For example, most people have very similar looking finger-tip blood flow wave forms, but a significant number of people may have a unique wave form pattern that easily discriminates them from the group.

Data from one of the physiological measures, the pressures applied to a computer mouse during the performance of a task of varying difficulty, has shown promise as a source of data for continuous identity authentication (“A User Identification Based on the Analysis of the Forces Applied by a User to a Computer Mouse”, Ikehara, & Crosby, 2003b). The pressure sensors are internally attached inside of a computer

mouse. The mouse has no outward appearance of being anything other than a computer mouse. The pressures applied to a computer mouse during clicking, was collected from six people during a pilot study. The potential of identifying a person with greater than 95% accuracy after two clicks was shown to be possible using discriminant analysis.

We have been using various physiological measures to identify different cognitive states “Real-Time Cognitive Load in Educational Multimedia” (Ikehara & Crosby, 2003a), “Model for Integrating an Adaptive Information Filter Utilizing Biosensor Data to Assess Cognitive Load” (Ikehara, Chin & Crosby, 2003), “Modeling and Implementing an Adaptive Human-Computer Interface Using Passive Biosensors” (Ikehara, Chin & Crosby, 2004) and “Methodological Issues of Real Time Data Acquisition from Multiple Sources of Physiological Data” (Vick & Ikehara, 2003). Our plan is to extract continuous identity authentication biometrics using similar methods we have used to extract cognitive states from multi-modal passive physiological sensor data.

### Applications

Two possible applications are described in the following paragraphs. The first application involves the higher security required to control access to the operation of high value vehicles such as cargo ships, container trucks and aircrafts. The critical security issue is that the authorized operator is controlling the vehicle at all times. The application of continuous authentication using multi-modal physiological sensors can help ascertain that the authorized operator is in control. For example, in an aircraft, a pilot's yoke and seat can be equipped with physiological sensors to allow the continuous authentication of the identity of the pilot. Initially, a pilot would register for access into the flight control system using a password, key or fingerprint. The multi-modal physiological sensors would then continuously authenticate who is piloting the aircraft. Should the pilot be displaced or incapacitated, an unauthorized user would be locked out unless a bypass procedure is performed, such as calling ground control to release access.

In this example, the multi-modal physiological sensors can be used to access two important secondary impacts regarding the control of an aircraft. The first is the health status of the pilot. Some of the sensors can give a clear indication of the health status of the pilot and alert either co-pilot or ground control of impending health issues that may not be apparent to the pilot and that can possibly affect control of the aircraft. The second is that some of the sensors can give an indication of the cognitive status of a pilot such as fatigue or excessive stress. The cognitive status must always be considered in the context of the pilot's activity (e.g., taking off, cruising or landing) and in the context of what is normal for the person (e.g., given the time of day or hours worked).

Another possible security application for a continuous identity authentication system (CIAS) using multi-modal physiological sensors would be when using critical computer systems. The initial registration of the user by password would be necessary, but by using a set of passive sensors built into a computer mouse, continuous authentication of the operator's identity would not interfere with the computer interaction. A computer system protected by the CIAS would have a limited number of registered users (e.g., usually one to three users). Initial access would not be

accomplished by comparing the user's biometrics to a large database of users (i.e., a one-to-many comparison), but by conventional high accuracy identification means such as a password or fingerprint. After initial access is obtained, continuous authentication of the user's identity would be performed by comparing the user's identity at initial access to the registered biometrics of that user (i.e., a one-to-one comparison). In many cases, a one-to-one comparison is faster and more accurate than a one-to-many comparison. A more detailed discussion of the differences and appropriateness of the one-to-one versus one-to-many comparison methods can be found in "Biometrics: Identity Verification in a Networked World" (Nanavati, Thieme, & Navanati, 2002).

The CIAS could be used with incident management software. Incident management software involves three primary functions: the input of an incident, the allocation of resources and the maintenance of the current status of the incident. Continuous identity authentication of the operator would be essential to guaranty the integrity of the incident management database and trust in the incident command center. An incident command center is filled with people from many different organizations. A false incident report resulting in the improper allocation of resources has several consequences. First, it would deplete resources for current needs. Second, trust in future requests will be diminished and may subsequently require multiple layers of authentication before a request is acted upon. Third, the incident management software database will need to be purged of false data which would negatively impact software operations.

Although the applications described above are very different, for both applications a CIAS would provide an added layer of security. Research is necessary to optimize the application of the CIAS technology.

### **Capabilities, Demonstrated Productivity and Experience of Applicants**

Curtis Ikehara is an assistant professor in the University of Hawaii Information and Computer Sciences Department. He is currently a researcher or co-PI on several projects. The current security related project he is involved in as a researcher is called, "Agent Based Modeling for Pacific Missile Range Facility Intent Analysis". This project, funded by the Office of Naval Research, is to develop algorithms that use information from a large array of sensors (e.g., video, LIDAR, RFID, seismic & infrared) to detect suspicious and threatening behavior of base personnel and visitors.

From 2002-2003, he was a co-PI on a DARPA project. The project focused on using physiological sensors with respect to applications in augmented cognition and the identification of cognitive processes. Dr. Ikehara and Dr. Crosby have developed a novel sensor, that measures the hand and finger pressures applied to a computer mouse and have applied for a patent for its use as a biometric device. In 2007, Dr. Ikehara and Dr. Crosby were awarded a US Patent for an "Input device to continuously detect biometrics" (US Patent # 7,245,218).

Both Dr. Ikehara and Dr. Crosby were presenters at the Biometrics Conference in Hawaii 2002, have presented conference papers on "User Identification Based on the Analysis of the Forces Applied by a User to a Computer Mouse" (Ikehara & Crosby, 2003), "Methodological Issues of Real Time Data Acquisition from Multiple Sources of Physiological Data" (Vick & Ikehara, 2003) and Continuous Identity Authentication Using Multimodal Physiological Sensors (Crosby & Ikehara, paper accepted to the SPIE

Defense and Security Symposium 2004, Biometric Technology for Human Identification).

## **Conclusion**

It's probably occurred to you that a finger print or an iris scan are more accurate or entering a password or using a key is easier. That's true, and in all high security applications at least one or more of these methods should be used, but these are point-of-entry deterrents, used upon initial access. What happens if you enter your password and someone knocks you on the head . . . they're into you secrets. Multi-modal continuous identity authentication using physiological sensors will prevent this problem by detecting an identity problem and asking for identity re-authentication, possibly by password reentry. Multi-modal continuous identity authentication can be unobtrusive and easy to use while continuously adding a layer of access security.

The continuous identity authentication system (CIAS) is one of a suite of crime prevention technologies that needs to be researched. CIAS has high and medium security applications, but before it is place into practice research is needed to evaluate the robustness of the identification process, user acceptance and the cost-benefit relationship.

## **References**

- Electronic Warfare Associates-Canada, Ltd. (2001). Biometric Technology Security Evaluation Under The Common Criteria, Communications Security Establishment Certification Body Canadian Common Criteria Evaluation and Certification Scheme.
- Ikehara C., Chin, D. N. and Crosby, M. E. (2004). A Modeling and Implementing an Adaptive Human-Computer Interface Using Passive Biosensors, Proceedings of the Hawaii International Conference on System Sciences, Kona, Hawaii (paper accepted).
- Ikehara C., Chin, D. N. and Crosby, M. E. (2003). Model for Integrating an Adaptive Information Filter Utilizing Biosensor Data to Assess Cognitive Load, Proceedings of the 9th International Conference on User Modeling, Pittsburgh, PA, June 2003.
- Ikehara, C. and Crosby, M. E. (2003a). A Real-Time Cognitive Load in Educational Multimedia, Proceedings of the 2003 World Conference on Educational Multimedia, Hypermedia & Telecommunications, Honolulu, HI, June 2003.
- Ikehara, C. and Crosby, M. E. (2003b). A User Identification Based on the Analysis of the Forces Applied by a User to a Computer Mouse, Proceedings of the Hawaii International Conference on System Sciences, Kona, Hawaii, <http://dlib2.computer.org/conferen/hicss/1874/pdf/187450130a.pdf>?
- Vick, R. M. and Ikehara, C. (2003). A Methodological Issues of Real Time Data Acquisition from Multiple Sources of Physiological Data, Proceedings of the Hawaii International Conference on System Sciences, Kona, Hawaii, <http://dlib2.computer.org/conferen/hicss/1874/pdf/187450129a.pdf>?
- Nanavati, S., Thieme, M. and Navanati, R. (2002). "Biometrics: Identity Verification in a Networked World", pp. 12 14.