Homeland Security

TechNote

Biometrics on CBRNE Watercraft

As the use of mobile computing, wireless networks, and cellular products expands into new applications and environments, law enforcement professionals have greater opportunity to employ wireless communications to remotely access data resources. Laptop and tablet computers with wireless Local Area Network (LAN) capability are often used by law enforcement agencies. The kinds of platforms on which these devices can be found range from a mobile vehicular command post to watercraft engaged in Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) detection and interdiction missions. Mobile computers used in emergency responder operations need to seamlessly access national databases and government wireless networks. Before access is granted, these resources often mandate the use of two factors of authentication. Two factors of authentication may include the use of a Personal Identification Number (PIN) and a token, such as a smartcard. Biometric technology can also be used as an authentication factor, alone, or in two-factor processes. The U.S. Attorney General requires Project SeaHawk, a collaborative local, state, federal anti-terrorist program in Charleston, South Carolina, to implement a two-factor authentication process in order to access federal data resources. This TechNote will define how biometric authentication technology can fulfill the federal requirements.

CBRNE Watercraft

Biometric Technology

Biometric authentication systems measure either the unique physical or behavioral characteristics of an individual seeking to gain system access. Biometric technologies represent an improvement in authentication capabilities because biometrics rely on something an individual IS rather than something an individual HAS or KNOWS. Token-based authentication relies on something an individual HAS, which can be lost, borrowed, or stolen. Access control through something an individual KNOWS, such as a password, is even less secure, because people often write down passwords and user names. This creates the same set of vulnerabilities found in token systems. Password access control systems are also vulnerable to "social engineering hacks" and keystroke loggers. Social engineering hacks are the equivalent of scams or cons

U.S. Department of Homeland Security

SAVER

System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security, Preparedness Directorate, Office of Grants and Training (G&T) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders in performing their duties. The mission of the SAVER Program is to

- Provide impartial, practitioner relevant, and operationally oriented assessments and validations of emergency responder equipment.
- Provide information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment.
- Assess and validate the performance of products within a system, as well as systems within systems.
- Provide information and feedback to the user community through a well-maintained, Web-based database.

The SAVER Program established and is support-ed by a network of technical agents who per-form the actual assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency respon-der community, "What equipment is available?" and "How does it perform?"

To contact the SAVER Program Support Office
Phone: 877-347-3371
E-mail: FEMA-ASKTS@fema.gov
Visit the SAVER Web site: https://
saver.fema.gov

aimed at information technology resources. Keystroke loggers record every keystroke a user makes, thus compromising PINs and passwords. Because they rely on unique human characteristics that cannot be passed on, biometric authentication systems eliminate these vulnerabilities.

Authentication

Authentication is defined as the procedure that determines an individual's identity, using either the identification or verification process. These processes represent the operational modes in any biometric system. Authentication begins when the individual's biometric data is presented to the system and a template is made from this extracted data. The identification process compares an individual's extracted template with many stored templates, in order to establish the identity of the user. The term "one-to-many" or "1:N" is often encountered in identification system literature. The process of identification answers the same question many times: Does this stored template match the individual's template? Verification is the process of matching an individual's extracted template against a single enrolled template in a database to assure user identity. An enrolled template is one that was acquired and registered in the database. The verification process only answers one single question: Does this template match the enrolled biometric template on file for the individual? Systems using the verification process save time by matching the extracted template to only one stored biometric template. Verification systems are also known as "one-to-one" or "1:1" systems. The identification process is useful in protecting certain resources from fraudulent use. The use of the verification process is more widespread because it is more rapid and allows a higher user throughput.

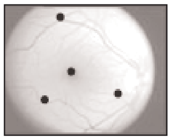
Biometric Logon Systems

As part of the authentication process, a biometric logon system requires a sensor that recognizes a pattern of unique physiological or behavioral characteristics possessed by an individual. The system compares the input template from the sensor, also called a scanner, with the template enrolled in a previously stored data file or on a token, such as an ID card. The database can be located at the scanner or at a remote security facility. Each of the biometric technologies listed in the next section (Biometric Technology Processes) could be applied to logical access control systems.

Biometric Technology Processes

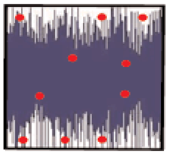
While there are many biometric technologies that can be utilized in law enforcement applications, the list narrows very quickly when considering the environmental range within which the biometric must function. CBRNE and security watercraft operate in, perhaps, the harshest environment within the emergency responder community. The watercraft environment includes wide variations in noise level, movement, saltwater spray, and extremes of temperature and humidity. In addition, user acceptance is an important issue for this select group of users. The device chosen must be perceived as a benefit or enhancement rather than a hindrance in an unpredictable tactical environment. It should be operable using one hand, with no peripherals or tokens, while the operator is engaged in other activities. The characteristics of some of the biometric technology processes that could be used in the CBRNE watercraft environment are briefly discussed below.

Facial recognition systems use one or more photographic images to recognize a person by measuring points on a face. Facial recognition technology is hands-free, but requires controlled environmental conditions using a firmly mounted camera to operate properly. This means that the camera location could impact computer mobility. Also, operation with the camera facing the sun, or in heavy spray or foggy condi-tions, can cause inconsistent performance.

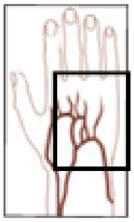


Retina scan and iris recognition systems require a mounted digital camera and controlled environmental conditions. In retina scanning, a visible light illuminates the retina (the back of the eye) from a close range. Retina scanning is perceived as intrusive because it can reveal information about medical conditions. Iris recognition employs a digital image of the iris (the colored part of the eye) taken from a distance of 3 to 18 inches and is considered very accurate.

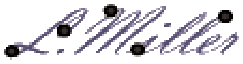
Voice recognition systems use the unique characteristics of human voice patterns to verify an identity and employ either a microphone or telephone to operate. As a person speaks, the vocal tract changes shape and those differing shapes contribute to the uniqueness of the voiceprint. Some systems measure the rhythm, tone, and pitch used by an individual to repeat one or more specific pass phrases. Variable ambient noise levels and voice changes under stress can affect reliable logon performance.



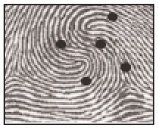
Vein, hand, and finger geometry systems rely scanner to capture the biometric sample. The scanner utilizes an infrared camera to focus on the face, wrist, or back of the hand to detect the unique pattern of veins located directly under the skin. Vein geometry is not intrusive and is extremely accurate, but requires a large scanner. Hand and finger geometry systems compare the shape of a user's hand or finger to a template stored in the database. Hand and finger geometry systems are not used for identification; however, they are most useful in verification.



Signature and keystroke dynamics require reproducible behavioral characteristics such as timing, shape, speed, stroke, or pressure in order to authenticate an identity. User acceptance is high with these systems and the equipment is not cumbersome. Providing a reproducible signature or keystroke, however, requires a stable environment. This biometric, therefore, is better suited to a bank lobby, point-of-sale, or clerical office environment.



Fingerprint biometric equipment is small, portable, and can be used for both identifi-cation and verification. Fingerprint features, called minutiae, are extracted by the fingerprint scanner. A complex algorithm is then used to extract a template for comparison to an enrolled template in the database. While performance can be affected by damaged, dry, or dirty skin on optical or capacitance fingerprint systems, new ultrasound technology in the biometric fingerprint industry can read most fingerprints regardless of these conditions.



All of the biometric technologies have advantages and disadvantages, but because highly accurate, rapid authentication is required under harsh environmental conditions, the fingerprint biometric may be the best candidate technology for use on mobile law enforcement computers. The scanner is small, easily wiped clean, and requires no other peripherals if a Personal Computer Memory Card International Association (PCMCIA) card is used, or an embedded fingerprint scanner is installed on the keyboard of the computer. The fingerprint biometric verification sequence is shown in Figure 1.

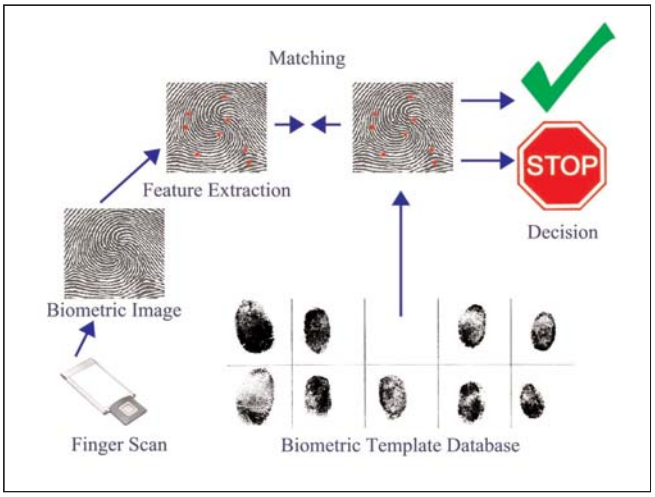


Figure 1 - Fingerprint Biometric Verification Sequence using PCMCIA Card

Biometric Performance Metrics

Vendors usually make claims regarding the performance of their sensors and equipment. These claims are based on performance metrics. Often, these metrics provide the sole source of objective information about the hardware under consideration. It is important to realize that the performance of any newly implemented system will rarely match claimed values. Once a system is deployed, performance metrics can serve as a guide for fine-tuning a biometric system. The following list provides the definitions of commonly encountered performance metrics.

False Acceptance Rate (FAR)/False Match Rate (FMR): The probability that an access control system will erroneously grant access.

Failure to Enroll (FTE): The probability that a user will be unable to enroll in a biometric access control process due to an insufficiently unique biometric sample.

False Rejection Rate (FRR)/False Non-Match Rate (FNMR): The probability that an individual's unique bio-metric sample or data will not be matched to the data in the access control system database.

Vendors use the FAR and the FRR as metrics for gauging the accuracy of their biometric systems. These metrics can vary depending on the sensitivity of the equipment that recognizes the biometric. FAR and FRR can be plotted on a graph to demonstrate the biometric system's performance at various sensitivity settings. Note that the FAR is equal to the FRR at the intersection point in Figure 2. The Equal Error Rate is the baseline for adjusting system sensitivity. Experience has shown, however, that a slightly higher FAR resulting in a lower FRR is preferred in computer logon devices. Furthermore, fingerprint analysis and other physical biometrics are generally more accurate than behavioral biometrics such as signature verification.

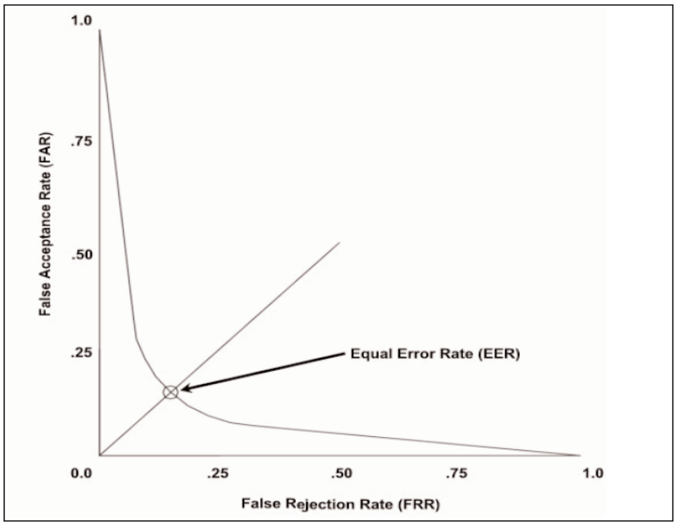


Figure 2 - Equal Error Rate

Conclusion

In order to gain high levels of user acceptance, the biometric authentication technology selected for access to a mobile computer in a CBRNE watercraft should be small, durable, require no other associated hardware or components to operate, and be seamlessly operable in tactical conditions. To eliminate conflict with platform controls and maintain functionality when the mobile computer is moved, the biometric device should be embedded in the mobile computer itself. In this way, the biometric capability can be utilized as another feature of the computer rather than an implementation of an additional level of access control. Market research indicates that fingerprint biometric sensors are small and durable enough to meet these requirements. Fingerprint sensors are available based on optical, capacitance, or ultrasound technologies, and are operated simply by touching or swiping a finger across the sensor. Visit the SAVER Program Web site at https://saver.fema.gov for more information on the SAVER Program or to view additional reports on biometric authentication technologies on CBRNE watercraft or other technologies.

This TechNote was produced through the efforts of SAVER technical agent, the Space and Naval Warfare Systems Center, Charleston.

SAVER is sponsored by the U.S. Department of Homeland Security, Preparedness Directorate, Office of Grants and Training, Systems Support Division.
Opinions or points of view expressed in this document are those of the authors and do not necessarily represent the view or official position of the U.S. Government.

For more information on the Biometrics on CBRNE Watercraft project please see the SAVER Web site or contact the SAVER Program Support Office.