Kristina Gebel

Andrew Wolfe

Cyber Security

27 July 2020

Behavioral Biometrics

Behavioral biometrics is the field of study related to the measure of uniquely identifying and measurable patterns in human activities. This focuses upon examining the non-biological or the non-physiological features of the human being.This is an innovative approach to user authentication that is based on the creation of a unique profile for each individual user. The term contrasts with physical biometrics, which involves innate human characteristics such as fingerprints or iris patterns. While behavioral biometric isn't necessarily new, the banking sector has been a part of this for many years, helping to provide convenient and robust authentication for online transactions, when combined with machine learning it provides a multi- dimensional profile for each consumer. Popular behavioral biometrics include, but are not limited to keystroke dynamics, gait biometrics, and hand gestures. Automatic recognition of people based on their anatomical (e.g., face, fingerprint, iris, retina) and behavioral (e.g., signature, posture) individualities is called Biometrics. It is a form of information that helps in identifying one's physical characters such as psychosomatic, behavioral characters, etc.

While biometric systems are less than perfect and mistakes can happen.

Biometric technology can provide a higher degree of security compared to traditional authentication methods. Chirillo stated that biometrics is preferred over traditional methods for many reasons which include the fact that the physical presence of the authorized person is required at the point of identification. This means that only the authorized person has access to the resources.

Effort by people to manage several passwords has left many choosing easy or general words, with considerable numbers writing them in conspicuous places. This vulnerability leads to passwords easily guessed and compromised. Also, tokens can be easily stolen as it is something you have. By contrast, it is almost impossible for biometrics data to be guessed or even stolen in the same manner as token or passwords. Nanavati was of the opinion that although some biometric systems can be broken under certain conditions, today's biometric systems are highly unlikely to be fooled by a picture of a face..." He further added that this is based on the assumption that the imposter has been able to successfully gather these physical characteristics which he concluded as unlikely in most cases.

One major reason passwords are sometimes kept simple is because they can be easily forgotten. To increase security, many computer users are mandated to manage several passwords and this increases the tendency to forget them. Cards and tokens can be stolen and forgotten as well even though attaching them to keyholders or chains can reduce the risk. Because biometric technologies are based on something you are, it makes them almost impossible to forget or manage. This characteristic allows

biometrics to offer much convenience than other systems which are based on having to keep possession of cards or remembering several passwords. Biometrics can greatly simplify the whole process involved in authentication which reduces the burden on user as well as the system administrator

Nanavati stated that "Biometric authentication also allows for the association of higher levels of rights and privileges with a successful authentication." He further explained that information of high sensitivity can be made more readily available on a network which is biometrically protected than one which is password protected. This can increase convenience as a user can access otherwise protected data without any need of human intervention

Disadvantages:

COMMON BIOMETRICS

Biometric technologies can either be physiological or behavioral. Physical biometrics includes fingerprint, facial recognition, hand geometry, iris scan, and retina scan. Voice recognition, signature and keystroke are all examples of behavioral biometrics. The commonly used biometrics are briefly described below.

FINGERPRINTING

"Fingerprints are the impressions of the papillary or friction ridges on the surfaces of the hand". He stated further fingerprints are the oldest and most widely recognized biometric markers. This statement is backed by Chirillo and Blaul who stated that

fingerprint recognition is one of the oldest biometric technologies. Lockie also stated that fingerprints are the most commonly used biometric.

Fingerprints have been used by humans for personal identification and access control for centuries. The matching accuracy using the biometric type has shown a very high figure. Fingerprints of even identical twins are different and so are the prints on each finger of the same person which increases the rate of accuracy.

According to postnote (2001), at a national level, automated fingerprinting is the only biometric used generally in the United Kingdom. An investigative project, which was to be completed by April 2002, was looking at the concept of using a single biometric identifier, likely to be fingerprints by default, throughout the Criminal Justice System including police, prisons and courts. Prisons already take ink fingerprints from convicted prisoners. These can be compared against the police database as proof that the right person is being held. An automated system would give rapid confirmation of a person's identity and allow Information about individuals to be shared quickly and easily.

When it comes to safety the first step is verification, and afterward, authentication is done. Generally, people use these two words interchangeably, but both the words have different meanings.

Authentication

- **Authentication refers to a process of determining that an individual is who only they claim to be.**

- **For example, asking dynamic Knowledge-Based Authentication questions that would be difficult for a different individual to answer. Generally to access bank statements you need to enter the account number as a password.**
- **For authentication, the individual has to answer specific questions to find out whether that person or individual is eligible to have certain rights to access this resource or not.**
- **Authentication takes confirmation to the next level and is especially important when we are dealing with online transactions.**

Verification

- **Verification means ensuring that the data is associated with a particular individual.**
- **For example, you are matching address or date of birth to an individual's name.**
- **For verification, the given data which is entered by an individual is matched with the previously stored information present in the database.**
- **Verification alone is required by some businesses and is merely an extra layer of security for others.**

Gait Biometrics

The interest in gait as a biometric is strongly motivated by the need for an automated recognition system for visual surveillance and monitoring applications. Recently the deployment of gait as a biometric for people identification in

surveillance applications has attracted researchers from computer vision. Gait Biometrics is based on the way a person walks. It is a behavioral type of biometrics. It does not get affected by the speed of the person's walk.

Advantages of Gait Biometrics:

- Can recognize a person at a distance where other biometrics are obscured.
- Effective where only low image resolution footage is available, as with CCTV cameras
- Non-invasive biometrics

Disadvantages of Gait Biometrics:

- It will not work if a person as worn an attire, such as a trench coat, or a footwear, such as flip-flops, that affects a persons walking style.
- Sometimes walking surface, downhill, uphill, etc could also cause a

Continuous authentication is possible using keystroke dynamics just as a mere consequence of people's use of computers. he basis of the biometric technology known as keystroke dynamics. Different people have different striking rate and style. It is analyzed and kept as a record for various security purposes.

Unlike many other biometrics, the temporal information of keystrokes can be collected to ascertain a user using only software and no additional hardware. The rhythm with which one types at a keyboard is sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics. Different people have different striking rate and style. It is analyzed and kept as a record for various security purposes.In summary, keystroke dynamics biometrics enables a cost effective, user friendly, and continuous user authentication with potential for high accuracy. Although keystroke dynamics is governed by a person's neurophysiological pathway to be highly individualistic, it can also be influenced by his or her psychological state. The rhythm with which one types at a keyboard is sufficiently distinctive to form

Signature recognition

Signatures have been in use from decades for personal identification as well as for high-value transactions. It is a behavioral characteristic and can produce a lot of statistically reliable data and also can be captured by electronic means. Earlier, manual methods of signature verification were used which includes confirmation of its shape. The biometric signature recognition system can verify a lot more to make sure that if it is an

authorized user or an imposter. Banks and financial service providers use signatures for authentication and authorization.

Voice recognition

Voice is a behavioral as well as a physiological trait that depends on the physical structure of the throat and mouth as well as chronic constituents. Being dependent on many factors, voice becomes a crucial biometric identifier which can be used to distinguish the speaker. Voice recognition recognizes the speaker as well as the speech. Speech recognition is an emerged technology-powered way of verifying what is being spoken, while speech recognition is about identifying who is talking, i.e., the identification of the speaker. Many people use speaker recognition and speech recognition interchangeably, but these two have different objectives, and approaches to implementation, except that both are related to human voice. A visual record of speech analyzed concerning frequency, duration, and amplitude is called the voice print or spectrogram. Voice recognition is very popular and low-cost, but it is less accurate and sometimes lengthy enrollmen

Works Cited

SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics Cheng Bo* , Lan Zhang† , Xiang-Yang Li* *Department of Computer Science, Illinois Institute of Technology, USA †Department of Software Engineering, Tsinghua University, China PR

BIOMETRIC AUTHORIZATION SYSTEM USING GAIT BIOMETRY L.R Sudha1 , Dr. R. Bhavani2 Department of CSE, Annamalai University, Chidambaram, TamilNadu

https://arxiv.org/pdf/1108.6294.pdf