Global Information Assurance Certification Paper

Social engineering defense using Biometrics

Mihwa Park
Jan. 4, 2002

Introduction

"Social Engineering" is an attempt by computer hackers to trick people into revealing their password or other valuable information [1]. Such attack is a single most efficient technique for attacking a company with good security systems. Also, this form of attack is difficult to defend against, and continues to grow steadily [1].

On the other hand, recently, the term "Biometrics" has been used to refer to the emerging field of technology devoted to the identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition [2].

Since biometrics is a field of study that recognizes a person using the distinguishing individual's characteristics, we can greatly reduce the chances of successful social engineering attack by utilizing those technologies. This paper explores possible defense techniques against social engineering by utilizing biometrics, particularly voice recognition technology.

Types of Biometrics Technology

In biometrics field, many types of biometrics systems have been developed and a few commercial products are beginning to appear in the commercial market, especially the security marketplace.

The type of available biometric systems are [3]:

- *Fingerprint Verification*
  Fingerprint verification technology is the most prominent biometric authentication technology, used by millions of people worldwide. Fingerprint Verification systems work by identifying the locations of small marks found in the fingerprint. Fingerprint readability is affected by a number of environmental factors, such as humidity, temperature, and so forth. False acceptance and rejection is estimated at around 0.0001% and less than 1% respectively.
- *Hand-based Verification*

Hand-based verification, also known as hand geometry, is a biometric authentication technology that dominates an important segment of the biometric industry - access control and time and attendance. Hand-based Verification systems are based on measurements of the geometry of an individual's hand. Some systems measure the geometry of two fingers. False acceptance is estimated at around 1 percent.

- *Retina and Iris Scanning*
  Retina scan is an exceptionally accurate biometric technology, having been established an effective solution for very demanding authentication scenarios. Iris systems also have the lowest false acceptance rates among all currently available biometric methods. Retinal scanning uses a very low intensity infrared camera to take an image of the back of the eye, while iris scanning works by identifying the unique patterns which constitute the texture of the iris. Even identical twins have different iris texture patterns, which remain the same throughout lifetime.
- *Dynamic Signature Verification*
  Dynamic Signature Verification system does not rely on its physical appearance but the manner in which a signature is written, using either a special pen or a sensitive tablet to track hand movements. However, some systems have difficulties with individuals whose signature changes substantially each type it is written.
- *Voice/Speaker Verification*
  Voice-verification is most often deployed in environments where the voice is already captured, such as telephony and call centers. Voice or speaker verification is a biometric authentication technology well suited for a handful of applications and systems in which other biometric technologies would be difficult to use. Making use of distinctive qualities of a person's voice, some of which are behaviorally determined and others of which are physiologically determined, voice verification is deployed in such areas as home imprisonment, banking, account access, home PC and network access, and many others.

Type of Voice Recognition Biometrics

Voice biometrics centered in the sound of the voice as generated by the resonance in the vocal tract. The length of the vocal tract and the shape of the mouth and nasal cavities affect the voice. Voice recognition is defined as the

automated process of identifying a specific individual's voice. In this case the sound signal is digitized and the digitized signal is compared to previously recorded samples held in a database. The result is a simple yes/no decision as to whether the speaker has been identified. Again, what is done with this information is dependent on the application(s) associated with the basic voice recognition application. A diagram of a typical voice recognition process is shown in Figure1 [4].

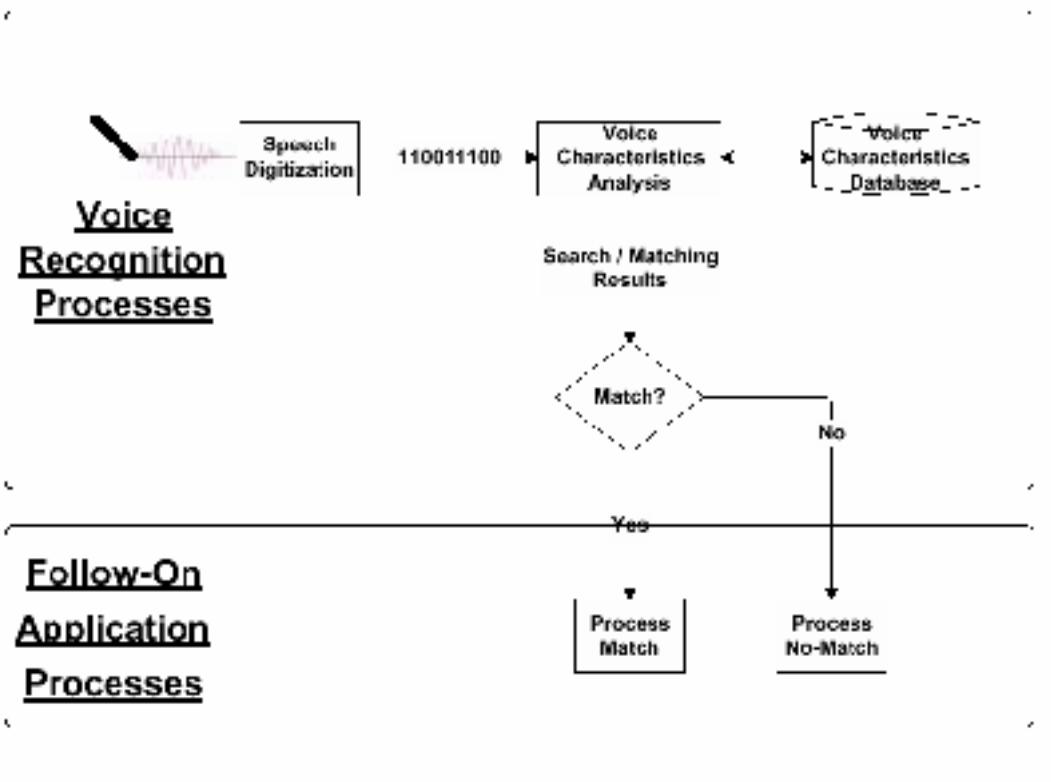

Figure1. Typical Voice Recognition Process*

*** This figure is excerpted form [4]**

Voice biometrics is classified into two specific categories : identification and verification [4]. Identification is the act of identifying individual and verification simply consists of confirming someone's identity. Compared with identification, verification is the more simple and reliable process. In voice identification biometrics, the identification is accomplished by comparing the spoken PIN (Personal Identification Number) or password to the individual's digitally stored voiceprint samples. These reference samples are previously digitized and

recorded words or phrases that are stored for later comparison to a live sample. Comparing and finding a match between an entry in the reference database and a live sample can successfully identify the individual. In voice verification, the voice characteristics of a speaker are compared to a reference sample in the database with a resulting right/wrong condition. Most voice verification systems allow for a keyboard-entered password as an auxiliary means of verification. This helps to avoid possible wrong conditions resulting from normal variations in a person's vocalization patterns that result from a cold, laryngitis, or any other reasons [4]. In a real world, voice verification is a real capability and is much more popular than voice identification. Voice verification has become a reality because of increases in processing power and improvements in algorithms . If same improvements occur with voice identification, the technology also will become more reliable and practical.

The advantages and disadvantages of voice recognition process are following:

Advantages

- Easy to use and require no special training or equipment. Users simply repeat phrases through a small microphone.
- Need not periodically manage/change his/her own password.
- Relatively inexpensive compared to other biometrics.
- Consumers prefer to use voiceprints than other biometrics for identification.

Disadvantages

- When processing a person's voice over multiple channels such as live through a microphone and over a telephone , the accuracy of matching is reduced.
- Physical conditions of the voice, such as those due to sickness, affect the voice verification process.
- Environmental problems reduce the overall accuracy of the device.
- Due to the volume of the voiceprint data, a large amount of computer storage space is required.
- One's voice changes over time , so matching is not always accurate.

Voice recognition products and corresponding vendors are shown in Table 1.

Product	Overview	Company
BioID [7]	BioID uses face, voice and lip movement recognition to identify a person for security and identification purposes	BioID
SpeakEZ Voice Print Speaker Verification [8]	The technology compares a digitized sample of a person's voice with a stored "voice print" of that individual's voice for verification.	T-NETIX Incorporated
VeriVoice Security Lock [9]	The VeriVoice Security Lock is a patented voice verification technology that provides a fast, highly accurate, and customizable solution for identification of enrolled users.	VeriVoice Inc.
VoiceCheck [10]	It handles all the enrollment, voice checking (verification), and database management needed to incorporate a voice verification solution	Veritel Corporation
CAS Guard [11]	Biometric authentication. Admin logon requires administrator to biometrically logon (using face, finger, or voice) before making changes and updates to the system.	Keyware Technologies
Speak N Set [12]	Designed for use with PC files. You can use a human voice as a password, as unique as a fingerprint, as natural as saying hello.	Veritel Corporation

Table 1. Voice Recognition Product & Vendors *

**** Table1's contents are briefly excerpted from [6].***

Conclusion

Many organizations have become more complex. But most users don't understand that their participation is necessary for security; users continually do foolish things: reveal his ID or Password; the threats are changing daily. The difficulty in securing your enterprise is no longer a technical problem. It is a social, political and cultural problem. So, organizations want to use a strong authentication model [13].

Biometrics, the automated measurement of a physiological or behavioral aspect of the human body for authentication or identification, is a rapidly growing industry. Also, biometric solutions are used successfully in various fields, such as e-commerce, network access, time and attendance, ATM's, corrections, phone banking, and medical record access. Ease of use, accuracy, reliability,

and flexibility are quickly establishing biometrics as the premier authentication technology. Also, the human voice is considered to be the most common form of communications and an ideal form of personal identification. Thus, the technique can be utilized in protecting someone from a social engineering attack. By utilizing such characteristics of biometric technologies, one can successfully protect networks from users who give out his or her password and prevent careless or unauthorized users from accessing many weak points in advance. Voice biometric devices are beginning to be seen in the marketplace, especially in security applications. They possess a promising future based on their ability to combine password protection and biometric verification in one process without requiring a keypad. Therefore, Voice biometrics can be an effective solution to human based social engineering.

References

[1] SANS, “The big picture: Social engineering ”, pp.18~20

[2] An Introduction to Biometrics, biometri c consortium http://www.biometrics.org/html/introduction.html

[3] Voice security system Inc, “Technology history”, http://www.voice-security.com/History.html

[4] SESA, “White Paper On Speech Recognition In The SESA Call Center”, pp.3~5

[5] Voice security system Inc, “Biometric technology”, http://www.voice-security.com/Biomet.html

[6] Biometrics Institute (The biometric resource center), “Product available for voice recognition”, http://www.biomet.org/voiceproducts.html

[7] BioID, “BioID products”, http://www.bioid.com/products/products.html

[8] T-NETIX, “SpeakEZ Voice Print speaker verification” , http://www.t-netix.com/SpeakEZ/default.asp

[9] VeriVoice, “VeriVoice products”, http://www.verivoice.com/products.htm

[10] Veritel Corporation , ”VoiceCheck software development kit”, http://www.veritelcorp.com/Products/sdk.html

[11] Keyware Technologies , “CAS Guard”, http://www.keyware.com/techsol/pages/casguard.asp

[12] Veritel Corporation , ”Speak N Set”, http://www.veritelcorp.com/Products/speaknset.html

[13] David Thompson , “The Social Engineering of Security” , http://www.eweek.com/article/0,3658,s%253D704%2526a%253D7263,00.asp