Safeguarding the Transmission of Biometric Measurements Used for Authenticating Individuals

Ernst L. Leiss
Ernst L. Leiss, Dept. of Computer Science, University of Houston,
coscel@cs.uh.edu

Abstract: Various biometric measurements can be used to establish the identity of individuals. Common to many of them is the fact that a significant amount of information is collected and transmitted; this information is then used to compare the captured biometric data with the previously recorded information identifying a particular individual. If the two pieces of information are similar, it is assumed that the identification is carried out correctly.

An important problem in this process is the safeguarding of the transmission of the captured information. In many cases, it cannot be assumed that the channel over which this information is transmitted is secure. Therefore it is crucial that the process be viable even if the channel is insecure. We outline an approach that ensures the security and integrity of this process. We demonstrate that this approach is highly effective in that it requires only minimal additional storage capacity and virtually no additional processing capacity to be functional.

Support of this research under NSF grants DUE 0313880, SCI 0453498, and OISE 0519316 is acknowledged.

1. Introduction

The authentication of users in shared systems is an important problem; it has numerous solutions [2, 3, 5, 10]. Historically, computer systems have used passwords to establish the bona fides of a would-be user. Passwords have a number of advantages and disadvantages. Among the advantages are the following:

Compactness: Extremely little information must be stored to carry out the identification process.

Universality: It is easy for anyone to invent a password.

There is an unlimited number of passwords.

Passwords can be retired and replaced at will.

The use of passwords is extremely efficient: Both providing new passwords and using passwords to verify identity is very fast.

Among the disadvantages are the following:

The connection between user and password is tenuous at best: There is no inherent connection between user and password, other than that the user invented the password.

Passwords are typically not unique: Many users tend to invent the same passwords.

While the compactness of passwords was an attractive feature for earlier computer systems, with their limited space, the disadvantages of passwords have provided the impetus for the study of alternative means for authenticating users. The most important of these are biometric measurements [8, 11].

Biometric measurements extract information that is tied directly to the physical properties or aspects of a user. They may be either entirely descriptive or capture abilities as well. Among the descriptive ones are fingerprints, retina scans, iris scans, hand geometry, face authentication, and DNA. Among those that capture abilities are signature-based verification, voice authentication, and methods based on keystroke dynamics. Common to all are the following features:

The biometric measurements are intimately tied to a specific individual.

They are more or less unique: Within reason, they uniquely identify a specific individual (see more specific discussion below).

The amount of data captured is significantly larger than that for passwords. Also, the amount of storage to accommodate the data against the captured data are compared is much larger.

Biometric measurement data must be similar to the stored data to generate a much. This is in marked contrast to the situation for passwords, where an exact match is required. In other words, biometric data require a **similarity** condition to be satisfied, while password schemes require a test for **equality**.

It is important to understand the implications of the similarity test, especially when contrasted with the equality test. While passwords are very definite, biometric measurements are inherently approximate; in most cases, there is a good deal of variability (of the objective aspects that are measured [most biometrics] or of the actual measurements [DNA]). Therefore, it is entirely inappropriate to apply a test for equality, which is of course precisely called for with passwords. Indeed, if one were to apply a test for equality in the context of biometric measurements to determine whether a match is present, virtually all tests would result in rejecting the authentication attempt.

Fingerprints [6] have been used for about a century to identify persons, primarily perpetrators of crimes. Fingerprints are generally assumed to be entirely unique.

However, not all individuals have suitable fingerprints, either because of missing fingers, medical conditions, or work-related abrasion. Typically, a great deal of fingerprint information is captured, but only certain aspects (called indicia) of the captured data are extracted and used in the similarity test. The amount of information used to establish valid matches (the number and type of indicia) varies.

Retina scans [7, 8] are based on the pattern of blood vessels in an individual's eye retina. The information contained in the measurements is generally considered to identify uniquely a given individual. The method is fairly intrusive and therefore not commonly employed.

Iris scans [8] are similar to retina scans and use the iris of the eye instead of the retina's blood vessel pattern; however, they are significantly less intrusive. They are considered to identify uniquely a given individual; even identical twins are said to have different iris scans. A substantial amount of data is captured which is then used to compute a similarity relation as basis for determining whether a match is present.

Hand geometry [4] uses geometric aspects of the hand and specific physical characteristics of hand and fingers. The data captured are either several 2D images or a 3D image. Again, a good deal of information is captured (approximately one hundred different measurements). However, it is not entirely clear how unique the resulting measurements are; typically, hand geometry is used to identify individuals drawn from a relatively small set (e. g., access control to a specific facility).

Face authentication [9] is easily the oldest technology for identifying individuals – of course not by computer, but by humans in their daily interactions. In the context of computer-based authentication, it is in fact one of the newest technologies. It measures geometric facial structure (distance between eyes, nose, mouth, jaw, etc.), either in 2D (not very reliable) or 3D. Measurements use either visible or infrared light (the latter being known as thermal imaging). The method is supremely non-intrusive; it is in fact the only biometric authentication approach that can be administered without knowledge and cooperation of the subject and also at a distance. A large amount of data is captured in this process. The similarity test is correspondingly complex.

DNA [1] is of course the ultimate identifier (except that it cannot differentiate between identical twins). While it has major drawbacks within the context of computer-based authentication, it shares with the other biometric approaches the aspect that a great deal of data must be captured in order to obtain enough of a basis to carry out a similarity test.

Signature verification [8] extends the classical signature approach (which only considers the final result, the signature) and includes information captured in the process of supplying the signature, such as pressure exerted on the surface during portions of the signature, variation of the angle of pen to surface for portions of the signature, speed of producing segments of the signature, and so on. Again, a good deal of information is captured which provides the basis for the similarity test against the stored template of information associated with a specific individual.

Voice authentication [7] employs specific characteristics of an individual's speech to identify that person. Because of the variability of a person's speech depending on factors such as medical conditions (cold, asthma, etc.) and fatigue, the similarity condition is especially crucial. Again, both the stored template (voice sample) and the captured voice record imply significant data requirements.

Finally, the (mechanical) way a user types text at a keyboard can be used to authenticate that user. While the discriminative power of keystroke dynamics [7] is limited (it is unlikely that millions of typists can be reliably differentiated from each other by this approach) and the failure rate is larger than with other biometric methods, it shares with them the fact that a substantial amount of data must be captured and transmitted in order to apply this approach.

A major disadvantage of all biometric approaches over password schemes is that it is (virtually) impossible to change biometric aspects of a person. In particular, this imposes dramatically more stringent security and integrity requirements on the operation of such methods, since it is not possible to "assign" to a human a new biometric measurement in case the original one was compromised. This is in marked contrast to passwords where the consequence of discovering the theft of a password is the issuance of a new one. This is possible because there is no tight link between the password and the individual. In the case of biometric information, this link is very tight and for all practical purposes indissolvable.

2. The Problem of Intercepts

We will assume in the following that sufficient security and integrity conditions are satisfied at the two endpoints of the process. In other words, we assume that the capturing device is reasonably secure and that the system involving the storage of the template and the processing of the similarity condition satisfies the requisite security and integrity constraints. This assumption is generally realistic because the two endpoints tend to be under the control of the agent interested in the proper functioning of the authentication process. Our specific concern for the purpose of this paper is with the transmission of the captured data.

The problem of intercepts can be stated as follows: Assume that biometric measurements of an individual requesting access are captured at an access point; these data are then transmitted to a central facility where it is determined whether a match between the captured measurements and the stored template exists. This involves carrying out the similarity test. If a match does exist, the individual is granted access; otherwise additional attempts may be permitted before access is definitively denied. The problem we address here is the following: How can we avoid that a third party intercepts the captured measurements for the purpose of reusing them at some other time and in an illicit way? While the inclusion of timing information may impede this replay attack, this is fraught with difficulties; in particular, this assumes that the measurement capturing access point is impervious to any attacks, in particular to schemes that cause it to change its local time. Since synchronization in this approach is crucial, the ability of the central processing facility to synchronize the times of the local measurement stations may be compromised and result in resetting the time, which in turn would defeat the approach using timing information to safeguard against replay attacks. This synchronization is needed more within the context of biometric measurements than for passwords because of the significantly larger amount of data transmitted. This is true even if the data to be transmitted are first encrypted (in this case the timing information would be part of the encrypted data).

3. The Proposed Solution

The problem of intercepts can be avoided by using the scheme described below. Here we assume that no reliable timing information is available. We require that the biometric measurements be encrypted before transmitting them, using some reasonably strong encryption method. An important implication of this assumption is the following [5,10]: Changing a single bit in the ciphertext (here the transmitted, encrypted measurement data) implies that the decryption of this modified ciphertext results in a plaintext that differs from the original plaintext in about half of all bits. In other words, a small change in the ciphertext will result in a huge change in the resulting plaintext.

We now exploit the fact that biometric measurements, in contrast to passwords, contain a great deal of redundancy: changing portions of a password most likely will result in another, valid password, while changing portions of biometric measurements will result in data that do not correspond to any real person. To put it differently, if we require passwords to consist of between 6 and 12 characters, using letters and digits, then there are more than four quintillion different passwords, even though there are fewer than ten billion persons; thus, each person would have almost half a billion passwords. On the other hand, biometric measurements may have a size of several hundreds to many thousands of bytes (that is, orders of magnitude more than passwords). Therefore, enormous redundancies are present in them.

It follows that because of the redundancy involved, because of the way measurements are taken, and because of the variability of human physical characteristics, no two different measurements are identical. This implies in particular that encountering identical measurements are an incontrovertible proof of a replay attack!

The leaves us with two issues to resolve: How to detect identical measurements, and how to ensure that attackers cannot produce artificially small variations in the measurements. The second question is easily addressed: Since the measurements are encrypted before transmission, the attacker has no access to the plaintext, but only to the ciphertext. Since a change in the ciphertext dramatically affects the resulting plaintext, such changes will result in (decrypted) measurements that are totally unrelated to the stored template. Therefore the match is guaranteed to fail.

Finally we come to the detection of identical measurements. Here, we assume that at the central storage facility, every successful measurement (i. e., every measurement that resulted in a successful match) is stored; then every subsequent access request consists of two parts, the test whether the measurement that was transmitted is identical to any previously transmitted measurement, and the similarity test as before. While the similarity test is most likely carried out on the basis of plaintext data (that is the transmitted encrypted data must be first decrypted), the test for equality can be applied either to cipherdata or decrypted data. (Recall that all modern password schemes operate exclusively on cipherdata!)

It is important to understand that the similarity tests involved in biometric data are quite complicated; in fact, some of the schemes mentioned above do not operate in real time, for this reason. An inherent problem is the fact that there is neither an order relation nor a proximity relation between the biometric measurements. (For example, there is no natural order of fingerprints in which "similar" fingerprints would be close to each other while dissimilar ones would be far apart.) However, the test for equality is extremely efficient: it is essentially binary search which runs in time proportional to the logarithm of the number of items to be compared against!

One problem with the above scheme is the amount of data that would have to be stored. Assuming that each measurement is 1kB, we would have to provide 1kB for each successful match. This may be considered excessive. However, it can be drastically reduced: Instead of storing the entire measurement data, we can apply a hash, such as MD5 or SHA [3,10], and reduce the amount of data to a significantly smaller amount. Given the random distribution of the hashes, it is reasonable to limit the size to fifteen bytes; this yields a space of potential hashes of size 2^{60}, or well over 100 sextillions (10^{20}), which is more than sufficient to differentiate between the fewer than ten billion humans alive. Yet, even if there are a million successful accesses in a year, the system requires additional storage capacity of no more than 150MB during a ten-year operation, a rather small amount in view of today's capacities of storage media.

It should be clear that the length of the hashes can be considered a parameter – if more space is available (or fewer access requests are anticipated), longer hashes can be used. Note that using a hash that is too short will (on average) result in more accesses being rejected as supposed replay attacks (a false negative, from the user's perspective). To illustrate this, assume the hash length were only one byte; thus, there are only 16 different hashes. Consequently, the likelihood that an access request is rejected as a supposed replay attack is 1 in 16. Note that in practice and given the characteristics of typical biometric measurement systems, once an access request is rejected as a replay attack, the individual requesting access is most likely asked to repeat the access request, generating a new set of biometric measurement data. Given the general nature of the processes, it is virtually inconceivable that this new set is identical to the previous one; in other words, the new data set is different if this is a legitimate measurement, and not a replay attack. Therefore, the likelihood of the second request being rejected again is greatly reduced, if it is legitimate! How many such repeat attempts are permitted is a policy issue. Important for us is that observation that repeated legitimate measurements necessarily result in different data sets being transmitted and compared against the stored template. This clearly enhances the usability of the approach without sacrificing any aspect of security of the overall system.

4. Conclusion

We have outlined an approach that safeguards against a replay attack within the context of using biometric data for authentication purposes. This scheme works in the absence of reliable timing information. It exploits intrinsic aspects of biometric measurements, namely their redundancy and their variability. The resulting method is highly efficient (it requires virtually no additional time to process the information, compared with the generic approach that does not safeguard against replay attacks); it also functions well with a relatively small amount of additional space.

Bibliography

[1] C. T. Clelland, V. Risca, and C. Bancroft. Hiding Messages in DNA Microdots. Nature 399:533-534, 1999.

[2] A. Conklin, G. Dietrich, and D. Walz: Password-Based Authentication: A System Perspective, Proc. 37th Hawaii Int'l Conf. System Sciences, 2004.

[3] S. Garfinkel: *Web Security, Privacy, and Commerce*, Second Edition, O'Reilly and Associates, Sebastopol, CA, 2002.

[4] Ingersoll-Rand Corp., IR Recognition Systems, last web site access 10 Aug. 2005, http://www.recogsys.com/company/index.htm.

[5] E. L. Leiss: *Principles of Data Security*, Plenum, New York, NY, 1982.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar: *Handbook of Fingerprint Recognition*, Springer, New York, NY, 2003.

[7] Microsoft informit.com, Access Control Systems, last web site access 10 Aug. 2005, http://www.informit.com/guides/content.asp?g=security&seqNum=149&rl=1.

[8] Z. Riha and V. Matyas: Biometric Authentication Systems, Tech. Report FIMU-RS-2000-08, Faculty of Informatics, Masaryk Univ., Hungary, Nov. 2000.

[9] T. D. Russ, M. W. Koch, and C. Q. Little: 3D Facial Recognition: A Quantitative Analysis, 38th Ann. IEEE Int'l Carnahan Conf. Security Technology, Albuquerque, NM, 2004.

[10] B. Schneier: *Applied Cryptography*, Second Edition, John Wiley and Sons, New York, NY, 1996.

[11] J. Woodward: *Biometrics and Strong Authentication*, Osborne/McGraw-Hill, Emeryville, CA, 2003.