Requirements for the Safe Transmission of Biometric Measurements for Authenticating Individuals

Ernst L. Leiss[1]

[1] Department of Computer Science, University of Houston, Houston, Texas 77204-3010, USA. Support of this research under NSF grants DUE 0313880, SCI 0453498, and OISE 0519316 is acknowledged.
coscel@cs.uh.edu

Abstract. An important problem in using biometric measurement for the authentication of individuals is the safeguarding of the transmission of the captured information. Often, the transmission channel is not secure. This is aggravated by the fact that the devices used to capture the information are unsophisticated; in particular, the devices tend to send information but do not engage in a dialogue necessary for an elaborate protocol. Of special concern is the "sniff and suppress" attack. We describe it and outline the requirements for avoiding it and similar attacks. Our conclusion is that existing biometric devices fall seriously short of these requirements and should be avoided until they are capable of establishing a multipass protocol that permits secure transmission of biometric measurements. We also outline an approach that ensures the security and integrity of this process.

Keywords: Biometric measurements, authentication.

1 Introduction

The authentication of users in shared systems is an important problem; numerous solutions have been proposed [2, 3, 5, 10]. The oldest approach in computer systems to establish the bona fides of a would-be user employs passwords. These have a number of advantages and disadvantages. Among their advantages are:

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 their disadvantages are the following:

The connection between user and password is very loose: 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 has been 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 essentially unique: Within reason, they uniquely identify a specific individual.

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

Biometric measurement data must be similar to the stored data to generate a match. 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 that similarity tests tend to be much more difficult (they are computationally more complex and error-prone) than equality tests.

The implications of the similarity test are profound, when contrasted with the equality test. While passwords are very precise, 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, a test for equality is entirely inappropriate, although this is 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.

Searching for a biometric measurement in a given set may be exponentially more difficult that searching for a password: Because of the identity test, binary search can be applied to passwords (if they are sorted, something that is easily implemented, at little additional cost since it occurs exactly once upon creation of the password, not every time access is sought), while the similarity condition for biometric data implies that a linear search is usually unavoidable.

In [12], we discussed a wide variety of biometric measurements, together with their characteristics. These include fingerprints [6], retina scans [7, 8], iris scans [8], hand geometry [4], face authentication [9], and DNA [1]. Signature verification [8], voice authentication [7], and the (mechanical) way a user types text at a keyboard (keystroke dynamics [7]) can also be used to authenticate a user. While the discriminative power of different techniques varies, from keystroke dynamics on one extreme to DNA on the other, all of them share the property that a substantial amount of data must be captured and transmitted in order to apply the approaches.

A major disadvantage of all biometric approaches over password schemes is that it is practically impossible to change biometric aspects of a person. 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 essentially 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 Simple Intercepts

In [12], we described a method that protected against simple intercept attacks. In this section we sketch this type of attack and the approach that safeguards against it. In the next section, we indicate why this approach does not safeguard against a slightly more sophisticated attack, the "sniff and suppress" attack. In all cases, our focus is on the insecure channel involved in the transmission. In particular, we assume that sufficient security and integrity conditions are satisfied at the two endpoints of the process [13]. Thus, the capturing device is reasonably secure and 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 simple 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 in eliminating simple intercept attacks 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, it 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).

The problem of simple intercepts can be eliminated as follows. Note that 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.

In defeating a simple intercept attach, we exploit the fact that biometric measurements contain a great deal of redundancy: changing portions of biometric measurements will result in data that generally do not correspond to any possible measurements of a real person. 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 can be identical. Therefore, encountering identical biometric measurements constitutes 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, 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 address the detection of identical measurements. We assume that at the central storage facility, every successful measurement (i. e., every measurement that resulted in a successful match) is stored; 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.

Note that the similarity tests involved in biometric data are quite complicated. 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.

The amount of data that needs to be stored can be significantly reduced by employing some type of hashing, for instance using MD5 or SHA [3,10]. This is explained in more detail in [12], as is the use of the length of the hashes as a parameter. However, this approach is susceptible to a “sniff and suppress” attack.

3 The “Sniff and Suppress” Attack

The “sniff and suppress” attack can be described as follows. Instead of a replay attack, the attacker sniffs the transmissions and determines when a biometric

measurement is transmitted. The attacker then suppresses this transmission, possibly replacing it with a completely random message that is guaranteed to be rejected. (Note that in a man-in-the-middle attack, the attacker would merely record the transmission, but pass it on. Here, the legitimate transmission does not get passed on, but is retained by the attacker.) The result of this action is that the attacker is now in possession of a legitimate set of measurements that has never been used to authenticate the user in question. It follows that the attacker is capable of impersonating that user, simply by employing this intercepted set of measurements. Since biometric measurements tend to be dependent on a multitude of factors, from environmental difficulties to the lack of precision with which users provide the data, it is much more common that an authentication request is rejected. For this reason, denying authentication, thereby requiring that the user repeat the process, is probably not very surprising. Therefore, this attack is unlikely to be detected. (We note that an initial objection to the approach proposed in [12] was voiced by an audience member when we presented it. The "sniff and suppress" attack is the result of refining this objection.)

It is clear that the intercepted data will permit the attacker only a single access. However, since the attack can be repeated several times, each time yielding a new set of valid and previously unused biometric measurements, this observation is of little help. In the next section, we provide a list of requirements that must be satisfied if one wants to use biometric measurements safely for authentication purposes.

4 Requirements for the Safe Transmission of Biometric Measurements over an Insecure Channel

We distinguish between systems that permit accurate synchronization and those that don't. While precise synchronization invariably involves a multipass protocol, it may be that synchronization is a basic operation supplied by the system. In all cases, our focus is on the security of the transmission over an insecure channel.

Systems with synchronization
In such systems, it is possible to use time-out features to eliminate the sniff-and-suppress attack. In other words, assuming fairly tight time tolerances, the attacker will not be able to complete the replay attack within the given limits. However, this may reject legitimate users as well if the transmission experiences delays of some type. Nevertheless, if the transmission time can be bounded from above by a very small constant, the sniff-and-suppress attack can be foiled. Since all other attacks are prevented by the method safeguarding against simple intercepts [12], this will be sufficient for secure transmission. Determining a workable value for this constant upper bound may however be a non-trivial problem, in view of the size of the data sets to be transmitted.

Systems without synchronization
In such systems, it will be necessary to employ a multipass protocol since the sniff-and-suppress attack cannot be timed out adequately. Specifically, there will be a need

for a hand shake in which the measuring device will have to request a unique piece of information that needs to be incorporated into the actual transmission of the biometric data. This piece of information must vary from one transmission to the next; additionally it may be necessary to establish at the central site a time-out mechanism, to the effect that a transmission is rejected after a certain amount of time, even if it involves the unique piece of information in the prescribed way.

Here is a possible realization of this approach. Let D be the device that captures the biometric measurements and let CS be the central storage site. Prior to the transmission of the biometric data, D and CS have agreed on the use of a specific encryption key K. When a user U attempts to authenticate herself, D first requests from CS an encryption key KU. The key KU is used only for this single authentication attempt; furthermore, the exchange between D and CS (D's request of KU and CS's response with KU) is encrypted using K. D then encrypts the previously captured biometric information of U using the encryption key KU and sends this ciphertext to CS. CS verifies that the process occurred within the established time limits and complies with all requirements. (Note that in this scenario, the simple intercept attack cannot be carried out since the key KU changes from one authentication request to the next.)

While this process safeguards against all possible attacks, it is not at all clear that devices used for capturing biometric information are capable to carry out this rather sophisticated protocol. The protocol requires precisely timed handshakes and must carry out encryption at various levels (one type of encryption for the protocol required for obtaining the key KU, another for the actual encryption of the biometric data). While the encryption involving the key K may well be public-key, it is likely that the subsequent encryption involving KU is some type of symmetric encryption, given the size of biometric measurements. (Note that public-key encryption typically requires time significantly above linear in the length of the message to be encrypted, while symmetric encryption virtually always works in linear time.)

There is no question that current generation biometric stand-alone devices do not have the capabilities required for these types of protocol and processing. The alternative approach, namely requiring precise synchronization between capturing device and central storage facility presents similar operational difficulties. At the same time, it should be glaringly obvious that absent safeguards against the sniff-and-suppress attack, a refinement of the man-in-the-middle attack, biometric measurements must not be used for the authentication of individuals. Recall that in contrast to passwords, it is practically impossible to obtain replacement biometric measurements associated with a particular individual.

We therefore conclude that current generation biometric stand-alone devices are inherently unsuitable for the authentication of individuals if data are to be transmitted over an insecure channel. This includes in particular any remote authentication based on biometric data that are transmitted over the Internet.

5 Conclusion

We discussed the difficulties involved in transmitting safely biometric measurements over an insecure channel. In view of the unique characteristics of such data, significantly more stringent security requirements apply than for passwords. We described in particular the sniff-and-suppress attack and concluded that any device able to foil such attacks must be capable of either precisely carried out synchronization or of carrying out multi-pass hand shake protocols. Since most of the current stand-alone devices for capturing biometric data do not satisfy this requirement, we conclude that such devices are inherently unsuitable for remote authentication where data are transmitted over general-purpose networks.

References

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, 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, 1982.
6. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar: *Handbook of Fingerprint Recognition*, Springer, New York, 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., 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, 2004.
10. B. Schneier: *Applied Cryptography*, Second Edition, John Wiley and Sons, New York, 1996.
11. J. Woodward: *Biometrics and Strong Authentication*, Osborne/McGraw-Hill, Emeryville, 2003.
12. E. L. Leiss: Safeguarding the Transmission of Biometric Measurements Used for Authenticating Individuals, Proc. IFIP World Computing Congress, NetCon, Santiago, Chile, August 20-25, 2006.
13. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996.