Authentication Techniques *

M. Esmaili, R. Safavi-Naini and Y. Zheng
The Center for Computer Security Research
University of Wollongong

1 Introduction

An important objective of security is to provide secrecy, i.e., to hide the contents of a publicly exposed message from unauthorized recipients. In contemporary private, commercial and diplomatic applications, however, it is frequently of equal or even greater concern that the legitimate receiver be able to verify that the message (information) has not been modified during its transmission or storage, or that it is not a counterfeit from an unauthorized transmitter. In some applications this requirement on the authenticity of information is of vital concern to all parties involved. For instance, in financial transactions the party who accepts a cheque usually insists on corroborating identification of the party who issues the cheque — authentication of the originator, or the transmitter, while the issuer not only fills in the face amount in numerals, but also writes out the amount in script, and may even go so far as to emboss that part of the cheque to make it more difficult for anyone to subsequently alter the face amount appearing on an instrument bearing his valid signature. Although this example illustrates the two main concerns of the participants in the authentication of information, namely, the verification that the communication was originated by the purported transmitter and that it hasn't subsequently been substituted for or altered, it fails to illustrate perhaps the most important feature in the current use of authentication. The information conveyed on the cheque is inextricably linked to a physical instrument, the cheque itself, for which there exist legally accepted protocols to establish the authenticity of the signature and the integrity of what the issuer wrote in the event of a later dispute as to whether the cheque is valid or the signature is genuine, independent of the information content (data, amount, etc.) recorded there. The contemporary concern in authentication is with situations in which the exchange involves only information, that is, in which there is no physical instrument that can later be used to corroborate the authenticity of either the transmitter's identity or of the communication.

The information to be authenticated may indeed be a message in a communication channel, but it can equally well be data in a computer file or resident software in a computer; it can be quite literally a fingerprint in the application of the authentication channel to the verification of the identity of an individual or figuratively a "fingerprint" in the verification of the identity of a physical object such as a document or a tamper-sensing container. In the broader sense, authentication is concerned with establishing the integrity of information purely on the basis of

*Prepared for the Australian Privacy Commission.

the internal structure of the information itself, irrespective of the source of that information.

In the simplest terms possible, *authentication* is nothing more nor less than the determination by the authorized receiver(s), and perhaps the arbiter(s), that a particular message was most probably sent by the authorized transmitter under the existing authentication protocol and that it hasn't subsequently been altered or substituted for. It should be obvious that an opponent should not, in all probability, be able to select a message that the receiver will accept as authentic, otherwise he could impersonate the transmitter and/or substitute fraudulent messages of his choice for the legitimate ones. The condition determining the set of messages the receiver will accept, and which the transmitter may use, are what specifies a particular authentication scheme. As we will see, this commonly involves some form of encryption/decryption operations, using secret keys, that enable the transmitter to construct a valid message and the receiver to verify the validity of the message.

2 Techniques Available

Cryptography provides an easy way for the transmitter and receiver to define a subset of valid messages that the transmitter can construct and the receiver can verify. Two types of cryptosystems are available:

i) Secret key cryptosystems, and

ii) Public key cryptosystems.

A more traditional technique that complements the two cryptographic methods is

iii) Biometric technique.

Biometric techniques limit access of unauthorized users and allow reliable user identification.

The rest of this report provides a full discussion of the three techniques for authenticating information.

2.1 Secret Key Cryptosystems

By a secret key cryptosystem, we mean a system that corresponds to the block diagram shown in Figure 1. The essential feature of such a system is the "secure channel" by which the secret key, K, after generation by the *key source*, is delivered to the intended receiver, protected from the prying eyes of the enemy. To emphasize that the same secret key is used by both the ecrypter and decrypter, secret key cryptosystems have also been called *one-key cryptosystems* and *symmetric cryptosystems*.

Perhaps the best example of secret key cryptosystems is the Data Encryption Standard (DES)[3, 4, 5]. In DES, the plaintext X, the cryptogram Y, and the key K are binary sequences with lengths $M = 64$, $N = 64$ and $L = 56$, respectively. All 2^{64} possible values of X are, in general, allowed. In its so-called *electronic code book mode*, successive 64-bit "*blocks*" of plaintext are enciphered using the same secret key, but otherwise independently. Any cipher used in this manner is called a *block*

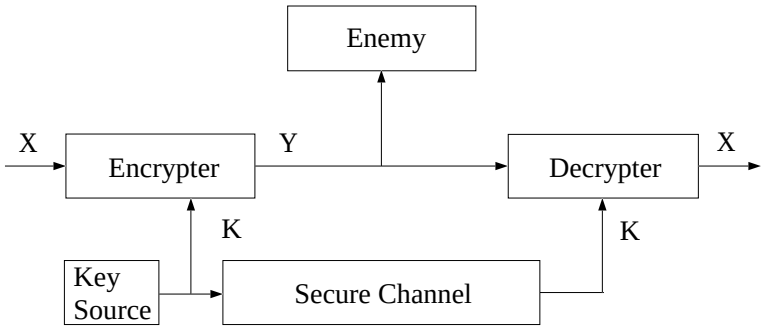


Figure 1: *Model of a secret key cryptosystem*

cipher. A block cipher algorithm can be used in different modes. The mode often used used for authentication purposes is *cipher block chaining mode*. In this mode the current block of plaintext is added (XORed) to the previous ciphertext block and then enciphered. This results in a strong dependency among the bits of ciphertext.

One way of authenticating a message, for example, is to append an authentication suffix (authenticator), which is usually obtained by appending a sequence of symbols to the message, and then encrypting the resulting extended message using a feedback chaining mode of a block cipher algorithm, so that the effect of the appended authenticator is spread throughout the resulting cipher. The resulting cipher is then transmitted as the authenticated message. The receiver, on receiving and decrypting the cipher using the secret key, accepts the message as genuine if and only if the cipher decrypts to a string of symbols with the proper authenticating suffix, and otherwise rejects it as unauthentic. In this example, the subset of messages (ciphers) that the transmitter will use and the receiver will accept are precisely those that have the authenticating suffix after decryption. If the cryptographic algorithm is secure, an opponent who doesn't know the secret key(s) being used by the transmitter and receiver can do no better than to randomly choose a cipher in the hope that it will be accepted by the receiver. If the authenticator is r bits, an opponent (if he cannot break the "sealing" encryption algorithm) would have only a 2^{-r} probability of choosing (guessing) a cipher that would be decrypted into a message ending with the unknown (to him) authentication suffix, and hence be accepted as authentic by the receiver.

This example illustrates an essential feature in all authentication schemes, namely, that authentication depends on the presence of redundant information, either introduced deliberately as in this example, or else inherently present in the structure of the message. This results is restricting the receiver and transmitter restricting to only a fraction of all possible messages, that is, to those messages containing this redundant information; any other messages would be rejected by the receiver as unauthentic. As used in this example, and in widespread cryptographic use, the term "authenticator" denotes the redundant information appended to the message that is to be authenticated. The object actually communicated by the transmitter to the receiver through the communications channel in this case is a "cipher". This use of the term "cipher" is in accordance with the accepted conventions of cryptography, since both the content of the original message and the authenticating redundant information must be concealed (kept secret) in the cipher, otherwise the appended authenticator, if it were revealed, could be used to authenticate an

arbitrary fraudulent message.

An equally common use of the term authenticator, with quite a different construction, is illustrated in the following example. To authenticate a message using DES or any single-key block cipher algorithm an authenticator, called message authenticator code (MAC), is constructed and is appended to the plaintext message. The authenticator is generated using cipher block chaining mode of DES. The information to be authenticated is first broken into blocks of 64 bits each. The first block is added bitwise modulo two (exclusive-or) to a 64-bit initial vector, which can be changed for every message, and the sum is encrypted using a secret DES key (known to both the transmitter and receiver). The resulting 64-bit cipher is then exclusive-or'ed with the second block of the text and the result is encrypted to give a second 64-bit cipher, etc. This procedure is iterated until all blocks of the text have been processed. The final 64-bit cipher is clearly a function of the secret key, the initial vector, and of every bit of the text, irrespective of its length. This cipher, called the Message Authenticating Code (MAC), is appended to the information being authenticated to form an extended message. The resulting extended message itself can be sent in clear, that is, unencrypted, although it may also be superencrypted if privacy is desired. The authenticator (MAC) can be easily verified by anyone in possession of the secret key and the initial vector by simply repeating the procedure used by the transmitter to generate it in the first place. An outsider, however, can not generate an acceptable authenticator to accompany a fraudulent message, nor can s/he separate an authenticator from a legitimate message to use with an altered or forged message since the probability of it being acceptable in either case is the same as his correct "guessing" of an acceptable authenticator, that is, 1 in 2^{64}. In this application, which is a classic example of an appended authenticator, the authenticator is a complex function of the information that it authenticates. The subset of acceptable extended messages in this case consists of those text-MAC pairs that pass the test of MAC being related to the text by the secret DES key. Since this makes up only 2^{-64} of all possible extended messages, the probability of an opponent being able to "guess" an acceptable message is less than his chance of "guessing" the secret DES key: 1 in 2^{56}.

In both of the above examples, the term "authenticator" denotes additional information communicated by the transmitter to enable the receiver to satisfy himself that the message should be accepted (as authentic). In the first case, the redundant information was appended to the message, and could therefore, if directly accessible to an opponent, be stripped off of a message and used to authenticate any other message. To prevent this, the resulting extended message was secured in a (block or feedback) cipher in which each bit of the cipher was a function of a secret encryption key and all the bits of the extended message. In the second case, the redundant information was already by virtue of the generating procedure, a function of the secret key and initial vector as well as all of the bits in the information being authenticated, and hence, with high probability, inseparable from the original text in the sense that it has no better chance of being accepted as the authenticator for some other text than would any other randomly chosen 64-bit sequence.

A problem inherently associated with authentication using a symmetric key system is that since both the transmitter and the receiver have the same secret key, cheating is unavoidable. In particular, the receiver can always produce a fraudulent message, with correct authenticator and then claim that he has received the message

from the other party. on the other hand the transmitter can deny at a later stage the fact that an authenticated message is originated from him. Section 2.2.1 provides a more detailed discussion of this problem. In the following we introduce public key cryptosystems and digital signatures that are ideal means of providing authentication when communicants are not trustworthy.

2.2 Public Key Cryptosystems

With the secret key cryptosystems came the problem of key distribution. If two people who have never met before are to communicate using conventional (secret key) cryptographic means, they must somehow agree in advance on a key that will be known to themselves and to no one else.

The second problem, apparently unrelated to the first, is the problem of signatures. Could a method be devised that would provide the recipient of a purely digital electronic message with a way of demonstrating to other people that it had come from a particular person, just as a written signature on a letter allows the recipient to hold the author to its contents?

On the face of it, both problems seem to demand the impossible. In the first case, if two people could somehow communicate a secret key from one to the other without ever having met, why could they not communicate their message in secret? The second is no better. To be effective, a signature must be hard to copy. How then can a digital message, which can be copied perfectly, bear a signature?

One solution to both of these problems is public key cryptosystems. Public key cryptosystems separate the capacities for encryption and decryption so that

1. many people can encrypt messages in such a way that only one person can read them, or

2. one person can encrypt messages in such a way that many people can read them.

This separation allows important improvements in the management of cryptographic keys and makes it possible to "sign" a purely digital message. In public key cryptosystems keys come in pairs. A pair consists of a *public key* and a *secret key* with the two following properties:

- A message encrypted with the public key can be decrypted with the secret key;

- Given the public key, it is infeasible to discover the other, the secret key.

This separation of encryption and decryption makes it possible for the users of communication system to list their public key in a *public directory* along with their names and address. A public key algorithm can provide secrecy and authenticity:

- **Secrecy**: a user can send a private message simply by looking up the addressee's public key in the directory and using it to encrypt the message. Only the holder of the corresponding secret key can read such a message; even the sender, should he lose the plain text, is incapable of extracting it from the ciphertext.

- **Authenticity**: a user can authenticate a message by encrypting it with his/her secret key. Anyone with access to the public key can verify that it must have been encrypted with the corresponding secret key, but this is of no help to him/her in creating (forging) a message with this property.

The best example of public key cryptosystems is the Rivest-Shamir-Adleman (RSA) system. The RSA system makes use of the fact that finding large (e.g., 200-digits) prime numbers is computationally easy, but that factoring the product of two such numbers is computationally infeasible. Alice creates her secret and public keys by selecting two very large prime numbers, P and Q, at random, and multiplying them together to obtain a *bicomposite* modulus N. She makes this product public together with a suitably chosen enciphering exponent e, but keeps the factors, P and Q, secret. To encipher a message M, one has to calculate $C = M^e \mod N$. The exponentiation modulo N can be carried out by anyone who knows N, but only Alice, who knows the factors of N, can reverse the process and decipher.

At present, the convenient features of public key cryptosystems are bought at the expense of speed. The fastest RSA implementation processes information at only a few thousand bits per second, while the fastest DES implementation does at many million.

2.2.1 Digital Signatures

There are many situations where the only security requirement is that the user (receiver) be confident that the stored information have not been altered and the identity of the provider of the information (sender) is not misrepresented. In other words, the user needs assurances concerning the authenticity of the information and of its origin.

One possible solution which has been discussed in the previous subsection involves the use of a conventional symmetric key cryptographic algorithm. In this scenario the sender uses the algorithm with a secret key, known only to the sender and receiver, to produce a message authentication code (MAC) or cryptographic checksum from the message.

This solution to the authentication problem is perfectly acceptable provided that the participants have faith in their ability to keep the key value secret and provided there is never a dispute between the two participants. Furthermore, it may also be sufficient to convince the receiver of the sender's identity. There is nothing, however, to prevent the receiver from changing the received message and then altering the cryptographic checksum or MAC so that it is authentic.

Similarly, there is no way to prevent the sender from claiming that he sent a message that is different to the one received. Thus there is nothing in this solution that prevents either parties from trying to cheat the other and, in the case of dispute, no evidence to enable a third party to settle the disagreement. The reason for this is that the cryptographic checksum or MAC depends on secret information that is shared by both parties and, therefore, either party can "imitate" the other.

If the two parties do not trust each other, as will certainly be the case if they do not even know each other, then the ability of one party to impersonate the other should be removed. Instead the sender is required to be able to "sign" the message in such a way that if anyone changes the message then the "signature" will reveal the fact that an alteration has occurred. Furthermore, if the signature is such

that it can not be "forged" then this will also authenticate the sender. The term "signature" here has been used deliberately because of the obvious analogy with written signatures.

In paper-based transactions the validity of a document is authenticated by a written signature. This signature then serves as an evidence of the signer's agreement to the authenticity of the information on the document and, furthermore, can be presented in court if the signer ever tries to deny agreeing to the statements on that document. The emergence of computer-based message systems has led to the need to find a digital equivalent of the written signature.

Properties of signatures. The crucial properties of a written signature are that it is easy to produce, easy to recognize but difficult to forge. It is this latter property that means that it cannot be repudiated and, as a consequence, written signatures are accepted as providing lasting evidence of precisely what has been authenticated and who has authenticated it. Digital signatures must have these properties of the written signature to be reliable for wide use.

Therefore, in an electronic system each user is required to be able to produce with ease a digital signature whose authenticity is easily checked. Moreover, such a digital signature must have the property that it could not have been produced by anyone else and can be used by a referee to resolve disputes.

Another fundamental property of a person's written signature is that it is the same on all documents. Although it may be a difficult task, a forger may, therefore, be able to learn from studying examples of the signature and so duplicate it (without detection). The security of a written signature lies in the difficulty of producing undetectable forgeries. In the case of a written signature, which is physically attached to a paper document, it is the ability to detect whether or not the document has been altered that guarantees that the document is one that was signed. On the other hand, since there is no physical way of determining how a digital signature was produced or what input was given and since a digital signal is easily replicated, a digital signature must be different for each message. It is the particular pattern of bits of each individual digital signatures that guarantees what message was signed and therefore, to prevent the substitution of an (altered) message to correspond to a signature, the signature must be a function which is dependent on all of the message. A forger, having seen many examples of a person's digital signature, should be no better informed as to how to produce a new (forged) digital signature of another message.

Since a digital signature is a message-dependent bit-pattern, the signing process must transform the message into the signed message (or signature). Furthermore, since the signature can only be computed by the originator, this transformation must use some information that is unique to the sender. As we saw in the last section, the public key cryptosystems can provide the required elements of digital signatures.

Authentication using digital signatures. Another possible way of authenticating a message is by signing it using a public key cryptosystem. As mentioned above, public key cryptosystems generally encrypt slower than conventional systems. Furthermore, some schemes produce signatures comparable in size to, and in some cases larger than, the messages they sign. This results in data expansion and effec-

tively lower bandwidth of transmission. Thus it is usually not desirable to apply a digital signature directly to a long message. On the other hand, we remarked that the entire message must be signed. This is seemingly contradictory, but a heuristic solution can be obtained by using a *hash function* as an intermediary.

2.2.2 Hash Functions

A hash function H accepts a variable-size message M as input and outputs a fixed size representation $H(M)$ of M, sometimes called a *message digest*. In general, $H(M)$ is much smaller than M; for example, $H(M)$ might be 64 or 128 bits, whereas M might have a mega bytes or more. A digital signature can be easily applied to $H(M)$ rather than M. The receiver calculates $H(M)$ using the received message M and the publicly known hash function H and validate the signature on $H(M)$ and then apply the public function H directly to M and check to see that it coincides with the forwarded signed version of $H(M)$. This validates both the authenticity of the origin and contents of M simultaneously. If $H(M)$ were unsigned only integrity of the content could be assured. A hash function must meet at least the following minimal requirement to serve the authentication process properly: it should be computationally infeasible to find a message that hashes to the same digest as a given message. Thus, altering a message will change the message digest. This is important to avoid forgery.

A hash function can also serve to detect modification of a message, independent of any connection with signatures. That is, it can serve as a cryptographic checksum (also known as a Manipulation Detection Code (MDC) or Message Authentication Code (MAC)). This may be useful in a case where secrecy and authentication are unimportant but accuracy is paramount. An important distinction is that a hash function such as a MAC used in connection with a secret key system is typically parameterized by a secret shared key, although the latter may be distinct from the session key used in transmitting the message and its MAC. In contrast, hash functions used in connection with public key systems should be public and therefore keyless.

2.3 Biometric Systems

One area where technology is enhancing, and often simplifying, our ability to identify people is *biometrics*. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physical characteristics, like a finger print or iris pattern, or some aspect of behavior, like handwriting or key-stroke patterns.

While biometrics is being applied both to identity verification and to identity recognition, the problems each involves are somewhat different. Verification requires the person being identified to lay claim to an identity, so that the system has a binary choice of either accepting or rejecting the person's claim. Recognition requires the system to look through large stored sets of characteristics of individual being presented, a more difficult task.

A range of biometric systems is in development or is available on the market, because no single system meets all needs. The tradeoffs in developing these systems involve component cost, reliability, discomfort in using a device, the amount of data needed, among other factors. Fingerprints, for example, have a long history of

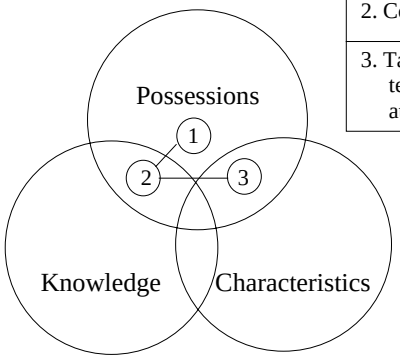
reliability, but the electronic imaging components required for capturing a fingerprint cost hundreds of dollars and the data describing a fingerprint, the template, is large. In contrast, the tools required to capture a signature–some sort of pen or stylus and tablet–are low in cost, and the template is very small; but signatures are not as stable as fingerprints, varying with people's emotional state, for example. Voice, too, is cheap to capture, relying on low-cost microphones or existing telephones, but varies when emotions and states of health change, and has a large template size.

2.3.1 Acceptability

Psychological factors also come into play when considering biometrics for different applications. Eye recognition, for example–both retina scanning, which requires close contact with the recognition device, and iris scanning, which can be done from a more comfortable distance–disconcerts some people because of an inherent protectiveness about their eyes. Quite the contrary, hand recognition, in which the palm is placed on a plate, appears not to bother people, perhaps because shaking hands is a common behavior. But in some applications, eye recognition psychological effect is a benefit–it appears to be a very serious recognition method and this seriousness may in itself discourage intruders.

Before looking at different biometric approaches, however, it is useful to understand the concepts of identification. A straightforward model of the process postulates three building blocks: something a person knows (a code), or possesses (a card), or has (a characteristic). From this static model a much more dynamic model for an identification scheme can be derived that balances such variables as types of threat, value being protected, user reaction, and of course cost (Figure 2).

Access to:	ID	Per-door cost	Asset value in dollars
1. General area	Smart card	$US400	Thousands
2. Computer rooms	Smart card and PIN	$US600	Millions
3. Tape vaults and telecommunications area	Smart card and fingerprint	$US5000	Billions



Most important requirements
Security levels
System throughput
User acceptance

Figure 2: *This system, which controls access to a credit card processing facility, employs not only fingerprint biometrics, but also a state-of-the-art card that attaches an integrated circuit chip to a plastic photo ID card. The chip stores the fingerprint image, the personal identification number (PIN), and security levels. The microprocessor in the card compares PINs and authenticates itself to the reader terminals. (Smart cards are the subject of another report.)*

Different situations warrant different approaches to identification. The three

basic ID methods may be combined to give varying levels of protection. The model can be changed by technology in two ways– automation and migration.

Automation may be applied to an existing process to reduce cost, improve quality, or handle higher volume. Today, for instance, picture ID badges, driver's licenses, and some bank credit cards are produced by electronic video-imaging systems instead of still cameras. Videocameras linked to PCs and modern color printers not only issue an ID credential, but also store the image in a computer. This processing hardly changes the behavior of the person being identified, who must still present his or her face and a credential to be identified; but it greatly enhances the ID operation.

While automation changes are generally internal to the organization and affect the identificand only slightly, migration affects both internal operations and the identificand. It occurs when the identification scheme is moved to a different section of the ID model. This move may be made to boost security levels, to speed throughput or capacity, to reduce cost, or to add convenience. Presenting a biometric X at an access point and requiring a PIN for credit card transactions are examples of new positions in the model. It means that care must be given to those who will be identified because their behavior is now being affected.

Biometric devices have three primary components. One is an automated mechanism that scans and captures a digital or analog image of a living personal characteristic. Another handles compression, processing, storage, and comparison of the image with the stored data. The third interfaces with application systems. These pieces may be configured to suit different situations. A common issue is where the stored images (reference templates) reside: on a card, presented by the person being verified, or at a host computer.

Recognition occurs when an individual's image is matched with one of a group of stored images. This is the way the human brain performs most day-to-day identifications. For the brain, this is a relatively quick and efficient process, whereas for computer to recognize that a live image matches one of many it has stored, the job can be time consuming and costly.

Most of the current biometric devices depend on a verification system, which requires the user to lay claim to an identity by presenting a code or a card. A formula or algorithm for matching two items then compares the live and enrolled images of the user's characteristic. The question by the machine is, "Are you who you say you are?" instead of "Do I know who you are?". Indispensable to all biometric systems is that they recognize a living person. One of the first questions newcomers to the field ask is, "What about a counterfeiting attempt using a latex finger, digital audio tape, plaster hand, prosthetic eye, and so on?" To prevent such fraud, many, but not all, devices include method for determining whether a live characteristic is being presented. The methods are sometimes ingenious but usually simpler than would be expected. Several companies are working on devices that will be very difficult to fool: for instance, an iris-scanning system soon to be released will look at characteristic pattern in the flecks of the iris, an infrared system for checking veins will look at flows of warm blood, and ultrasound fingerprint readers will look at subcutaneous structures.

2.3.2 Technology available

Biometrics encompasses both physiological and behavioral characteristics, (Figure 3). A physiological characteristic is a relatively stable physical feature such as a fingerprint, hand silhouette, iris pattern, retina pattern, or facial feature – all these are basically inalterable without trauma to the individual.

A behavioral trait, on the other hand, has some physiological basis, but also reflects a person's psychological makeup. The most common trait used in identification is a person's signature. Other behaviors used include a person's keyboard typing and speech patterns. Because most behavioral characteristics change over time, many biometric machines that rely on behavior update their enrolled reference template each time they are used. After many successful accesses, the template may differ significantly from the original data, and the machine become more proficient at identifying the person. Behavioral systems work best with regular use.

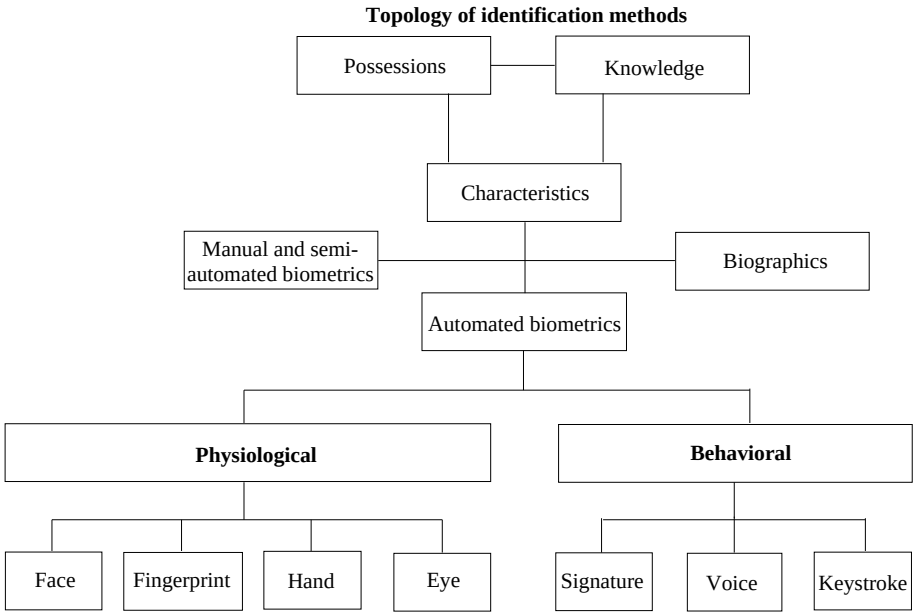


Figure 3: *Personal characteristics–physiological and behavioral–may serve as the basis biometric identification. Physiological characteristics vary little from time to time, but their use may be considered threatening in some applications. Behavioral characteristics may be hard to measure because of influences such as stress, fatigue, or colds, but they seem more acceptable to users and generally cost less to implement in a system.*

The difference between physiological and behavioral methods are important. For one, the degree of intrapersonal variation is smaller in a physical characteristic than in a behavioral one. Barring injury, after all, a person's fingerprint is the same day in and day out, whereas a signature is influenced by both controllable actions and unintentional psychological factors.

The most commonly discussed measure of a biometric's performance is its identifying power. This measure is defined by a slippery pair of statistics known as false rejection rate (FRR) and false acceptance rate (FAR). To set the desired balance of FAR and FRR, many machines have variable thresholds. If this tolerance

setting is tightened to make it harder for impostors, some authorized people may find it harder to gain access. Conversely, if it is easy for rightful people to gain access, the frightful may slip through. On the first attempt, a user typically has to sacrifice some false rejection to get near-perfect protection against impostors.

Although developers continue to work on techniques to reduce FRR, improvements become more elusive as the percentage of problem cases falls. Most early adopters of biometrics have found that training people in using the machines effectively is the best way to reduce false rejections. Most have also found that false reject rates drop markedly after two weeks of use.

Identification systems on the market or in development today employ a variety of biometric approaches. Hand geometry is the eldest ancestor of biometrics by virtue of its 20-year history of live application. Another approach is using fingerprint which is gaining popularity for general security and computer access control applications. Two other methods of identification involve the eye, scanning the blood vessel pattern on the retina and examining the pattern of the structure of the iris. Biometric developers have also not lost sight of the fact that humans use the face as their primary method of telling who's who. Another biometric approach that is attractive because of its acceptability to users is voice verification. All the systems used in analyzing the voice are rooted in more broadly based speech-processing technology. Also signature dynamics, because of its promise for automating the job of verifying signatures in the financial community, has been one of the hottest areas of biometric development. Keystroke dynamics, also known as typing rhythms, is one of the most eagerly awaited of all biometric technologies in the computer security.

3 Comparison

The following table compares different methods of authentication.

	Secret-key Cryptosystems	Public-key Cryptosystems	Biometric Systems
Speed	High	Low	High
Memory Requirement	64 bits for secret key and 64 bits for Initial Vector	400-500 bits for secret key and a trusted data base for public keys	9 bits to megabytes depends on the application
Reliability	Good	Very good	Good (despite some rejections)
Security Level	High	High	Reasonable
Cost	Not much	>$1000	$600-$70,000
Convenience	Convenient	Convenient	Not in all applications
Availability	Export restrictions	Export restrictions	Available

4 Security of Personal Information Databases

As was explained in the previous sections, the memory requirements for different methods vary. For example, when the DES, a symmetric key encryption algorithm, is used in authentication, an individual user only needs to store 64-bit secret key and/or 64-bits for the initial vector, whereas an organization such as a bank which can have hundreds of thousands of clients or users, may need a huge data bank that stores 128 bits for each client. For public key systems this requirement is much higher; each user has to store his/her secret key and there must be a complete directory of public keys which should be maintained by a trustworthy authority and be available to all potential users. With biometric techniques, the memory requirement for an individual user varies from zero to a few mega bytes in a smart card, while the requirement for an organization which has a large number of clients can be a huge data bank. For each client there is an entry in the data bank which stores the biometric information, such as fingerprint features, of the client. To protect the sensitive authentication information stored in organizations' data banks special data handling systems called data bases are employed.

Generally, a *data base* is a collection of *data*, such as personal information, and a set of *rules* that organize the data by specifying relationships among the data. Through these rules, the user describes a *logical* format for the data. The data are stored in a file, but the precise *physical* format of the file is of no concern to the user. A *data base administrator* is a person who defines the rules that organize the data and also controls who should have access to what parts of data. The user interacts with the data base through a program called a *database manager* or a *data base management system* (DBMS) – informally known as a *front end*.

The following is a list of requirements for security of data base systems.

- *Physical data base integrity*, so that the data of a data base is immune to physical problems, such as power failures, and so that it is possible to reconstruct the data base if it is destroyed through a catastrophe.
- *Logical data base integrity*, so that the structure of the data base is preserved. With logical integrity of a data base, a modification to the value of one field does not affect other fields, for example.
- *Element integrity*, so that the data contained in each element is accurate.
- *Auditability*, to be able to track who has accessed (or modified) the elements in the database.
- *access control*, so that a user is allowed to access only authorized data and so that different users can be restricted to different modes of access (for example, read or write).
- *User authentication*, to be sure that every user is positively identified, both for the audit trail and for permission to access certain data.
- *Availability*, meaning that users can access the data base in general and all the data for which they are authorized.

Integrity. The integrity of elements of a data base refers to their correctness and accuracy. Ultimately, authorized users are responsible for putting correct data into data base. However, users make mistakes collecting data, computing results, and entering values. Therefore, the DBMS must be able to help a user detect errors as they are entered and correct errors after they are inserted.

The DBMS maintains the integrity of each item in the data base in three ways. First, it can apply *field checks*, which are tests for appropriate values in a position. The check ensures that a value falls within specified bounds or is not greater than the sum of the values in two other fields. These checks prevent simple errors as the data are being entered.

Integrity is also maintained by *access control*. A data base may contain data from several sources. Prior to development of data base, redundant data might have been stored in several places. When data changes, each separate file requires correction. Data bases have led to the collection and control of this data at one central source. This makes it easy for the user to be sure of having the correct data.

However, ownership of a shared central file is a question. Who is authorized to update which elements? What if two people apply conflicting modifications? What if modifications are applied out of sequence? How are duplicate records detected? What action is taken when duplicates are found? These are policy questions that must be resolved by the data base administrator.

The third means of maintaining the integrity of a data base is to maintain a *change log* for the data base. A change log is a list of every change made to the data base; the log contains both original and modified values. With this log a data base administrator can "undo" any changes that were in error.

Auditability. In some applications it may be desirable to generate an audit record of all access (read or write) to a data base. Such a record can help to maintain the integrity of a data base or, at least, to discover after the fact who had affected what values and when. A second advantage is that users can build up access to protected data incrementally: no single access reveals protected data, but a set of accesses taken together reveals the data like the clue to a mystery. In this case an audit trail would be useful to identify which clues a user already been given, as a guide to whether to tell the user more.

Access control. The data base administrator specifies who should be allowed access to which data, at the field, or record, or even element level. The DBMS must enforce this policy, granting access to all specified data or no access where prohibited. Furthermore, the number of modes of access can be many. A user or program may have the right to read, change, delete, or append to a value, add or delete entire fields or records, or reorganize the complete database.

User authentication. The DBMS may require rigorous user authentication. For example, a DBMS might require a user to pass both specific password and time-of-day checks. This authentication is in addition to authentication performed by operating system. Typically, the DBMS runs as an application program on top of the operating system. This means that it has no trusted path to the operating system, and it must be suspicious of any data it receives, including user authentication. Thus the DBMS must do its own authentication.

Certain characteristics of the user, external to the data base, may also be considered. To enhance security, the data base administrator may permit x to access the data base only at certain times, such as during working hours. Another characteristic to be considered is previous requests of the user. Sensitive data can sometimes be revealed by combining results from several less sensitive queries.

Techniques described in Section 2 can be employed to add security and authentication to every field, record, or even elements in data base of personal information.

References

[1] *Contemporary Cryptology: The Science of Information Integrity*, edited by Gustavus J. Simmons, IEEE Press, 1992.

[2] B. Miller, Vital signs of identity, *IEEE Spectrum*, February, 1994.

[3] *Data Encryption Standard (DES)*, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, Apr. 1977.

[4] *Guidelines for implementing and using the NBS data encryption standard*, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 74, National Technical Information Service, Springfield, VA, Apr. 1981.

[5] *DES modes of operation*, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 81, National Technical Information Service, Springfield, VA, Dec. 1980.