The Generation of Biometric Digital Signature

Andru Putra Twinanda

Informatics Engineering, School of Electrical Engineering and Informatics, Institut Teknologi Bandung
Jl. Dago Asri D19, Bandung, West Java
e-mail: ndrewh@yahoo.com

Abstract *– A digital signature or digital signature scheme is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type.*

It is highly required that the private key is unique and unknown. Because of this need, biometric digital signature is introduced. There are a lot of parts in human body that can distinguish one from another, such as fingerprint, DNA, and retina. By using appropriate device and software, we can generate a digital signature from the uniqueness of human. Implemented well, this could revolutionary change the whole perspective of digital signature because of its ease of use.

Key Words*: digital signature, biometric,*

1. INTRODUCTION

A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, Digital Signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

Digital signature implements the asymmetric cryptography which requires two kinds of keys, public key and private key. The private key is secret and held by the one who wants to sign a document and the public key is not secret, so everyone may have this key.

The private key, as stated before, has to be secret and no one may have it in order the digital signature provide non-repudiation service. And also it has to be unique. Many researchers have thought of a way to provide both needs, and that's why biometric digital signature is introduced.

It is a common sense that there so many physical things in human body that distinguish one from another, such as fingerprint, DNA, and retina. If information from the things that make us unique can be extracted then the security in digital signature can be gained.

2. DIGITAL SIGNATURE

2.1. Main Idea

The main idea of digital signature is signing a document with something that can be verified at side of the one who will receive the document. As stated, this requires two keys, private key held by the one who signs the document and public key held by the one who will receive it.

2.2. Implementation

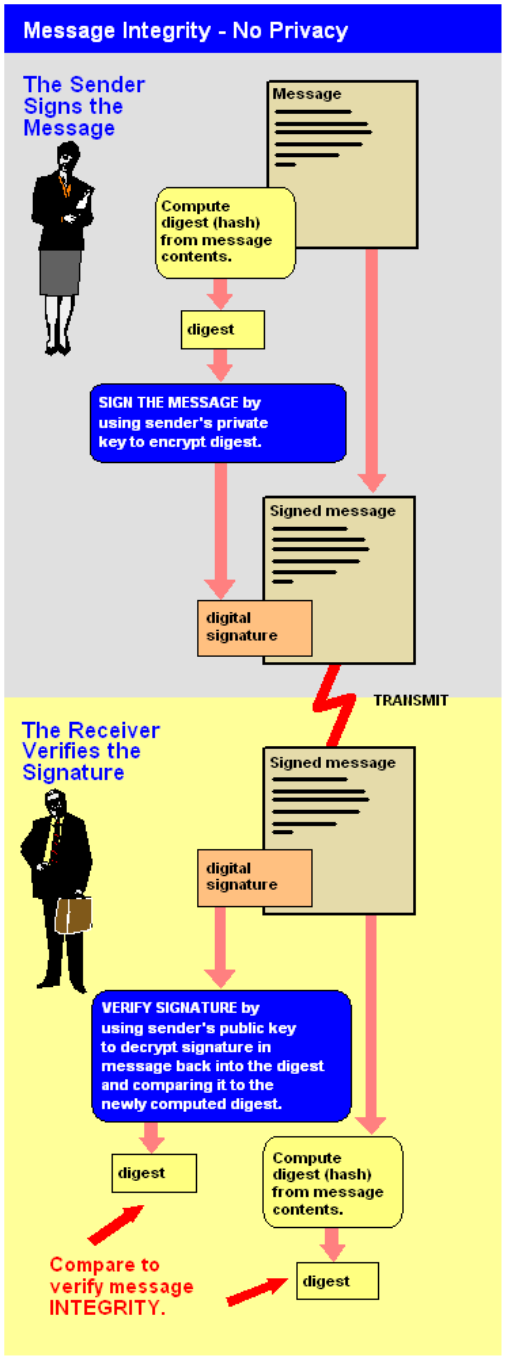

Figure 1 Digital Signature Work Flow

As shown in Figure 1, the message that's going to be sent will be computed with a hash function creating a message digest. The message digest serves as a "digital fingerprint" of the message, if any part of the message is modified; the hash function returns a different result. Then, the message digest will be encrypted with a private key. This encrypted message digest is the digital signature for the message.

The sender sends both the message and the digital signature to the recipient. When the recipient receives them, the signature will be decrypted using the public key, thus revealing the message digest. To verify the message, the message will be hashed with the same hash function used by the sender and compares the result to the message digest. If they are exactly equal, the recipient can be confident that the message is originally sent from the sender and has not changed since it was signed. If the message digests are not equal, the message either originated elsewhere or was altered after it was signed.

Note that using a digital signature does not encrypt the message itself. If the sender wants to ensure the privacy of the message, she must also encrypt it using the recipient's public key. Then only the recipient can read the message by decrypting it with his private key.

It is not feasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto the signature. Specific hash functions have been designed to have the property that finding a match is not feasible, and are therefore considered suitable for use in cryptography.

3. BIOMETRIC DIGITAL SIGNATURE

3.1. The Main Idea

One inevitable drawback of the cryptographic schemes is that the signer must carefully hold and possess a signing key which is not memorable at all. It is desirable occasionally to derive the signing key from a human source, say biometrics, rather than keeping it in an external hardware device. Biometrics is actually the science of using digital technologies to identify a human being based on the individual's unique measurable biological characteristic such as fingerprint, voice pattern, iris pattern, face, retina, handwriting, thermal image, or hand print. It is widely recognized that automatic

identification is the most suitable application for biometrics. In some sense, the digital signature can be compared to a biometric signature that is verified by capturing a real hand-written signature. However, it is technically hard to apply biometrics directly to the digital signature because of its inaccurate measuring and potential hill-climbing attacks.

3.2. The Requirements

Some drawbacks of deriving a unique deterministic value such as a private key from one's biometrics only are that:

a. the derived value is to be obsolete once the biometric template is compromised
b. the possible number of keys are limited exactly by the number of biometrics enrolled by the user
c. the compromise of biometric template eventually implies the permanent corrupt of the user's corresponding biometrics.

As for the compromise, a potential biometric vulnerability known as a *hill-climbing attack* should be given extra attention. This attack could occur when an attacker has access to the biometric system and the user's template upon which the attacker wishes to mount a masquerade attack. The attacker could exploit the compromised biometric template to produce a new image that exceeds the threshold of the biometric system and use that image again as input to the system to which the original template belongs. The private key can be derived so easily.

As a result, there are two critical requirements for generating a digital signature using biometrics. They are to randomize the signing key derived from biometrics and to keep the biometric template from hill-climbing attackers. However, it has been accomplished that the secure hardware storage is not provided for users. So it is needed to explore a different model where user's biometrics are acquired but randomized for deriving a signing key and user's biometric templates are resistant to their exposure, without any provision of the secure hardware storage devices.

3.3. The Implementation

There are two Sejong University students, T. Kwon and J. Lee, who have developed a way in order to make biometric digital signature and minimizing all the disadvantages that it has.

First, it is required to look at the definitions of:

a. **Security Parameters.** Denoted as κ and l where κ is a general security parameter and l is a special security parameter for public keys.
b. **Digital Signature Scheme.** Formally a digital signature scheme is denoted by

$$\Sigma = (G\Sigma\,(1^l),\ S,\ V)$$

where $G\Sigma$ is a probabilistic algorithm returning a public-private key pair from input 1^l, and S and V are respectively signing and verifying algorithms, which run in polynomial time.

a. **Public Key Infrastructure.** For an authorized assertion about a public key, digital certificates issued by a trusted entity called the certificate authority (CA) are used in the existing public key infrastructure (PKI).

In order to generate a digital signature using biometrics without smart-card like devices, it is stated that the human users can be scanned with regard to their biometrics and some personal possession that is not protected directly by hardware. So a user is defined formally as $U = \{B,P\}$ where B and P mean respectively user's biometrics and possession. We can regard B as a probabilistic algorithm returning user's biometrics while P is deterministic.

Given a signature scheme Σ, we have to manipulate the key returned by G_Σ to be linked with both the user's biometrics and possession. So the following transformation is defined:

$$T_1 = <G_\Sigma(1^l),\ G_R(1^\kappa), B> \rightarrow <B_T, P_T>$$

$$T_2 = <B,\ B_T,\ P_T> \rightarrow G_\Sigma$$

where G_R is a probabilistic algorithm returning a random integer from input 1^κ, and B_T and P_T are respective transformed values. Then $P = \{B_T, P_T\}$ is defined. As a result, T_2 implies that both B and P, say only a user, can derive the corresponding key generated in T_1. From the perspective of biometrics, T_1 is for enrollment while T_2 is for verification. Similarly, from that of digital signature, T_1 is for initial key generation and key hiding while T_2 is for key recovery and signature

generation. Note that it is required that both transformation should be easy to compute but respective inverse transformation must be computationally infeasible. So, it is impractical for our transformation to measure *B* by feature extraction which cannot guarantee enough entropy.

In this formal model, *U* can be interpreted as an oracle that returns an output *B* probabilistically to query Q_B, and an output *P* deterministically to query Q_P. So we could model the attacker *A* who is capable of asking Q_P only to *U* with regard to the hill-climbing attack. It is obvious that *P* can be released from a hardware device and the hill-climbing attack is still defeated in our model if *B* is only acquired in a legitimate phase. Similarly an attacker who acquired a sample of *B* cannot proceed with generating a digital signature without obtaining *P*. This could be a standard consideration of two-factor security. Then all we have to do is exploring suitable techniques or tools that satisfy our model.

One of the tools that can be used to satisfy the model explained before is image processing**.** Since it is not easy to derive a cryptographic key from varying biometrics, much work have been done in practice to use an independent, two-stage process to first authenticate the user through biometrics and then release the key from hardware storage. However, very recently, an innovative technique that links the key with the biometric at a more fundamental level during enrollment and then retrieves it using the biometric during verification has been developed by C. Soutar [2].

It is interesting to process the entire fingerprint image rather than doing feature extraction, in the way that seemingly our transformation can be satisfied. So their scheme are carefully investigated and concluded that the so-called biometric encryption scheme satisfies our formal model in implementing transformation T_1 and T_2. The main reason is that it provides distortion tolerance to accommodate the day-to-day distortion of the fingerprint image, discrimination to distinguish the aimed one clearly from other fingerprints, and security to extract independently neither the cryptographic key nor the legitimate fingerprint from the stored data that can be queried by Q_P in our formal model. During enrollment, a secure block of data called a Bioscrypt is generated by T_1, while it can be combined with the biometric image sample for T_2 during verification.

4. CONCLUSION AND SUGGESTION

4.1. Conclusion

Digital signature is needed to verify whether a document is original or has been edited. The drawback of the conventional way of digital signature is the owner has to hold it in a safe place, so any people won't find out about the key. Unlike the conventional way, biometric digital signature doesn't require much attention from the owner because it's already in the body of the owner.

Although it is very practical and easy, biometric digital signature still has many disadvantages. They are the inaccuracy in measuring and the vulnerability against hill-climbing attack.

Biometric digital signature can substitute the usage of conventional digital signature once the proper way to keep the key has been found and the vulnerability against hill-climbing attack has been solved.

4.2. Suggestion

In order to introduce new things in digital signature field, biometric digital signature should be introduced in the class and it should be in the curriculum of Cryptography lesson. By learning the biometric digital signature, students would know how well it has been developed, how it is implemented and how the prospect is in the future.

5. BIBLIOGRAPHY

1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Penerbit ITB 2006

[2] C. Soutar, "Biometric system performance and security," http://www.bioscrypt.com/assets/biopaper.pdf, 2002