24

SAND98-0989C
SAND--98-0989C
CONF-980534--

On Enabling Secure Applications Through Off-line Biometric Identification

George I. Davida
Univ. of Wisconsin-Milwaukee
Milwaukee, WI
davida@cs.uwm.edu

Yair Frankel
CertCo LLC
New York, NY
yfrankel@cs.columbia.edu

Brian J. Matt
Sandia National Laboratories*
Albuquerque, NM
bjmatt@cs.sandia.gov

Abstract

In developing secure applications and systems, the designers often must incorporate secure user identification in the design specification. In this paper, we study secure off-line authenticated user identification schemes based on a biometric system that can measure a user's biometric accurately (up to some Hamming distance). The schemes presented here enhance identification and authorization in secure applications by binding a biometric template with authorization information on a token such as a magnetic strip. Also developed here are schemes specifically designed to minimize the compromise of a user's private biometrics data, encapsulated in the authorization information, without requiring secure hardware tokens.

In this paper we furthermore study the feasibility of biometrics performing as an enabling technology for secure system and application design. We investigate a new technology which allows a user's biometrics to facilitate cryptographic mechanisms.

1 Introduction

Secure digital identification schemes are becoming increasingly important, as more security applications require identification based on physical characteristics rather than solely on a user's knowledge of a secret cryptographic key or password. The increased interest in such applications, ranging from door access to electronic commerce applications, has led to an increased interest in methods for secure and accurate identification [8, 5, 18, 17] of individuals as well as machines and objects. In this paper we are interested in systems of identification that use measurable biological features, biometrics, which can be readily measured at the point of application. It is desirable that such measurements be non-invasive and simple to perform. One biometric that has been suggested is the iris scan [3, 12, 6, 21].

On-line applications secured through the use of biometric authentication typically are based on a push or pull model. In both models, the first step is a user initialization, which occurs when the user's biometric template is registered with the on-line server. After initialization, when a user wants access that requires biometric identification, a *biometric authorization process* is performed. At this time the user's biometric is read by a reader. In the push model, the reader transmits (preferably via a private channel) the reading to the on-line server; the on-line server then verifies the validity of the reading based on the user's template in the server's directory; and finally the server sends an authenticated acceptance or rejection message back to the reader. In the pull model, the reader requests the template from the server, and the reader performs the verification steps after receiving the template over an authenticated and, preferably, private channel from the server. In both cases, an authenticated channel is necessary for some communications between the on-line database and the reader. The authentication can also provide for a binding of a user's biometric with some form of authorization, as established by trust relationships between the reader and the on-line database.

Here we are interested in developing biometric based identification systems which do not require the incorporation of an on-line database for the security infrastructure. Such databases are not always practical in mobile environments, such as military applications, and are often cost prohibitive since they require expensive wiring for connectivity or costly wireless devices. In order to remove the connectivity requirements, an *off-line* biometric system is achieved by incorporating a biometric template on a storage device / token (e.g., magnetic strip or smartcard) which provides for a reliable storage medium; however, there are no security requirements required of the token. We, therefore, will work in the pull model with the storage device containing sufficient information to validate the authenticity of the user's acquired biometric template to the biometric generated during user initialization. To provide for the user biometric/user authorization binding, a trusted authorization officer who authenticates (signs) the user's biometric template is incorporated into our infrastructure.

A biometric identification system which provides

*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

the user's biomeric template in the clear may not be acceptable to a user, because a user's biometric template could be used for unacceptable purposes if the template is obtained by an unauthorized individual. Biometric templates can provides information which a user may not want provided readily. For instance, a finger print reading can be used for law enforcement purposes and an eye scan (retinal or iris) may be able to detect medical conditions.

We study the feasibility of protecting a user's biometric on an insecure device. Such protection may be beneficial if the storage device holding the biometric template is lost or stolen. This added protection may provide for stronger user acceptance, since the user's template is not sent in the clear. In our study we propose a classification of secure off-line biometric systems according to who, if anyone, in the system has a private decryption key (when templates are encrypted).

An important model to consider is the case where *neither the user nor the reader* maintains private decryption keys, because it is a scalable solution when the user must have authorization amongst multiple readers and when password protection is inappropriate. Providing for authorization bound to a biometric template appears to be inherently difficult in this model, because the user's biometric template cannot exist in the clear on the storage device.

To achieve our result we had to overcome several hurdles. The first is to deal with errors which occur during the reading of biometrics. Variances from multiple readings of the same user often occur due to problems such a scratch on a finger, disease affecting blood vessels in the retina, variations in light causing changes in the pupil size during iris reading, and different positioning of the object being scanned (finger, head, etc.). In an off-line system if there are any discrepancies between the original template and later readings, the biometric template cannot be verified against the authentication officer's authentication information.

Another hurdle that had to be overcome is that cryptographic authentication mechanisms (e.g., a digital signature) that the trusted authorization officer invokes to bind authorization with a user's template do not necessarily hide all the information of the input (i.e., provide confidentiality of the message that is signed), thereby potentially leaking information about the user's biometrics. Let us give an example of a signature scheme SIG which leaks the acquired message completely. Let $sig(m)$ be the signature of a message m; observe as a simple example that one can generate a new secure (unforgeable) signature function $SIG(m) = (m, sig(m))$, (e.g. message/signature pair $(m', (m, sig(m))$ is valid if $m' = m$ and $Verify(m', sig(m)) = TRUE$). Hence, signature functions do not necessarily protect against information leakage of the input. A solution to this problem is simple, of course, if the trusted authorization officer and reader share a private key.

It should be noted that our system is also applicable to on-line systems where information is stored in an on-line database instead of on storage cards. By using our system in an on-line environment, one is able to reduce the security requirements imposed on the database. For example, our techniques prevent the database manager from reading biometric templates directly from the database or archives.

We also note that designers of secure systems are often hampered by the lack of mechanisms to satisfy the various requirements of a secure key management infrastructure. This infrastructure may have to deal with generation of both public and private keys, authenticated dissemination of keys, and the storage of keys, as well as other concerns such as maintaining privacy of users and trusted circulation of user authorizations. The security of this infrastructure is often hindered by insufficient mechanisms to secure private keys for users. We noticed that when one assumes that a user's biometric information has sufficient uncertainty, our technique also allows for the biometric template to be used as a private key. Since there may not be sufficient entropy (i.e., uncertainty) in a user's biometric, our system allows us to augment password encryption with the entropy provided in a biometric.

Our solutions are based on cryptography. We do not assume unproven, and usually expensive, physical protection mechanisms such as optical computers (see [20]).

The result we present here has many features:

- We present off-line identification systems based on any biometric technology that can be measured accurately (up to some Hamming distance).
- Enhancements also allow for incorporation of authorization information from a trusted authorization officer. In essence our system binds the user identity not only for simple access but for authorization.
- We classify off-line biometric systems according to which entity (e.g., reader, user, authorization officer), if any, must maintain a long term private decryption key for the purpose of hiding a user's biometric from compromise.
- Based on our classification of off-line biometrics, we discuss the feasibility of designing a system in which information stored in the the storage device does not compromise the biometric information of the individual involved when a card is lost or stolen.
- The techniques presented provide for on-line identification systems in which the privacy of a biometric template is protected on the database.
- We propose an infrastructure and mechanisms which allow biometrics to enable cryptographic applications when there is sufficient entropy in a user's biometric.
- In presenting our results, we shall relate them to the iris technology[3, 12, 6, 21].

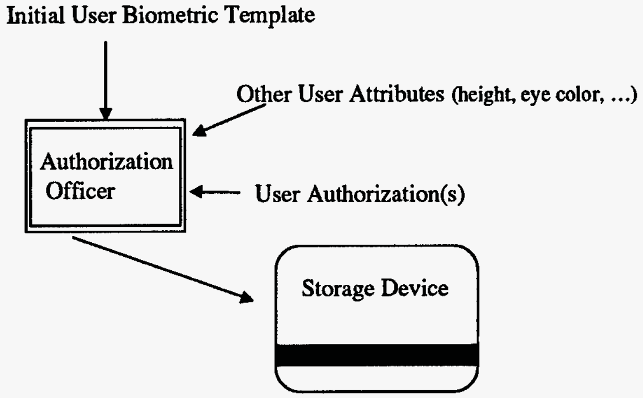
Initial User Biometric Template
Other User Attributes (height, eye color, ...)
Authorization Officer
User Authorization(s)
Storage Device

Figure 1: Storage device initialization

2 Model

We shall propose several models in which off-line biometrics can be incorporated into a security infrastructure. In order to motivate the design of our off-line system, we first analyze in Section 2.1 how an on-line system would work and the requirements which may be desired for such a system. We then investigate in Section 2.2 the off-line model for access control, authorization and private key storage.

In our models below we use an authorization officer entity in the architecture. The authorization officer's role is to certify (e.g., authenticate or sign) a binding between a user's biometric template and some other attributes of the user. The authorization officer is thereby the trusted third party attesting to authorization as well as to other user attributes. The authorization officer plays a role that is similar to the Certification Authority (CA) in a public key hierarchy (see [22]), except that the authorization officer binds biometrics to user attributes, while a CA binds a public key to user attributes.

In considering biometrics, we note that we need to make the following assumption:

Assumption 1 (Reproduction): *We assume that a biometric is not reproduceable. Hence it is unique to an individual, but even more importantly, one should not be able to artificially generate a "device" with sufficient characteristics to pass a biometric verification of a user.*

This assumption must be achieved in any high consequence application protected by a biometric system, in order to provide secure and unique identification. Otherwise, an adversary with sufficient probability will be able to impersonate a user by reproducing the authorized user's biometric. To provide for such protection, properties such as pupillary unrest of an iris and blood flow and heat from a finger scan have been used to support this assumption in some biometric systems. Throughout this paper we assume the biometric system we incorporate into our designs provides sufficient protection to provide the reproduction assumption.

2.1 On-line Model

Our architecture for an off-line system is motivated by the on-line system. We first briefly review the model for an on-line system.

The primary application of biometrics today involves the use of an on-line server. During *system setup* biometric readers are connected to a trusted on-line server through secure links which are either cryptographically secured channels or in which physical security is established. If cryptographic security is used, then a secure key distribution is required.

User initialization is performed by the user having his/her biometric template registered with the on-line server. Later, when a user wants access which requires the user to pass through a biometric identification, a *biometric authorization process* is performed. The user first has his/her biometric read by a reader; the reader transmits the reading to the on-line server; the on-line server then verifies the validity of the reading based on the user's template in the server's directory; and finally the server sends an authenticated acceptance or rejection message back to the reader. This is the push model for an off-line system. In the pull model, the reader requests the template from the server, and the reader perform the verification steps, after receiving the template over an authenticated and, preferably, private channel from the server.

Our off-line model below is inspired by the pull model. It simulates the on-line transmission of a user's template to the reader with storage device containing a user's biometric (or similar information) for verification authenticated by an authorization officer's signature.

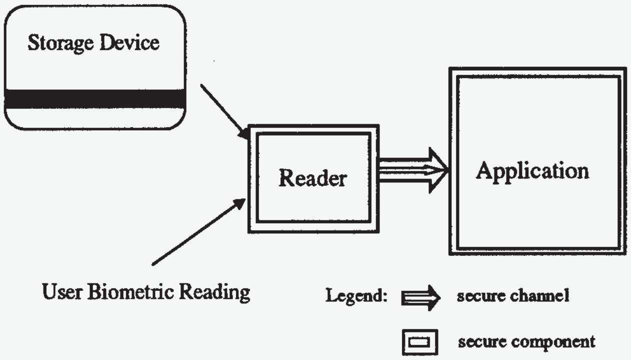

Figure 2: Secure application with biometric authorization

2.2 Off-line Model

In the off-line system, the biometric authorization process cannot have a direct (on-line) information retrieval mechanism. This requirement means that the push model cannot be used, because it requires a communication from the reader to the on-line database and back. The pull model, however, can be simulated by incorporating a storage token which replicates the information sent by the on-line reader. We should note, however, that as with any off-line identification system, immediate revocation of user privileges is not possible. This limitation must be taken into consideration by the system designer during the development of the security architecture.

We now discuss the workflow in the off-line model.

Initialization process:

The user initialization process for the off-line model is represented in Figure 1. The secure authorization officer takes as input an initial biometric reading, called the user biometric template, the authorization information defining the set of privileges granted the user by the authorization officer, and other user attributes. As output a storage device such as a magnetic strip card is encoded with information which establishes a binding between a user's biometrics (and, possibly, other user attributes) and the user's authorization granted by the authorization officer.

Application process:

During a secure application, as depicted in Figure 2, a reader takes as input the user's storage device (token) and reads the user's biometric. Given this information, which may also include other user attributes not represented in this figure, the user's authorization attributes can be obtained and linked to the authorization officer. This information may now be securely transmitted to the secure application. Note that the primary difference between an off-line and on-line system is that the storage device can be replaced by an authenticated transmission link to the authorization officer (or its database) in the on-line system.

Certain principles are incorporated in our model:

1. There must be a binding between a user's biometric and a trusted authorization officer. Hence, we require a storage device (e.g., magnetic strip or smartcard) to store the binding information.

2. There is a need for a scalable solution when privacy of a user's biometric must be protected in case a storage device is lost or stolen. The primary scalability issues are who must store private keys and how much storage must be provided on the cards.

Principle 2 suggests an interesting feasibility question. Is it possible to provide a scalable solution and protect a user's biometric, and if so, what requirement must be imposed on the security architecture? To answer the question, we now classify the off-line security architectures by who, if anyone, must hold a private key.

Private key in reader: If a reader has a private key to decrypt biometric information encrypted by the authorization officer, then there will be no leakage of biometric information when a card is lost or stolen. However, such a system is not scalable if the memory device has low storage capability and the application's architecture requires multiple readers (each with its own private key), because a separate encryption of the biometric template is required for each reader. This technique however, can be effective if there are few readers in the architecture.

In Figure 3 we show the information that must be stored on a storage device when multiple readers are used.

To be effective, this approach requires that the readers provide some form of protection for the reader's private key (e.g., FIPS PUB 140-1 standards [9]), because if the private key is stolen from

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.