EXHIBIT 23

BIOMETRIC AUTHENTICATION — SECURITY AND USABILITY

Václav Matyáš and Zdeněk Říha
Faculty of Informatics, Masaryk University Brno, Czech Republic
{matyas, zriha} @fi.muni.cz

Abstract We would like to outline our opinions about the usability of biometric authentication systems. We outline the position of biometrics in the current field of computer security in the first section of our paper. The second chapter introduces a more systematic view of the process of biometric authentication – a layer model (of the biometric authentication process). The third section discusses the advantages and disadvantages of biometric authentication systems. We also propose a classification of biometric systems that would allow us to compare the biometrics systems reasonably, along similar lines to Common Criteria [1] or FIPS 140-1/2 [4]. We conclude this paper with some suggestions where we would suggest to use biometric systems and where not.

Keywords: authentication, biometrics, classification, evaluation, security.

1. INTRODUCTION

This paper summarises our opinions and findings after several years of studying biometric authentication systems and their security. Our research on security and reliability issues related to biometric authentication started in 1999 at Ubilab, the Zurich research lab of bank UBS, and has been continuing at the Masaryk University Brno since mid-2000. This paper summarises our personal views and opinions on pros and cons of biometric authentication in computer systems and networks.

Proper *user identification/authentication* is a crucial part of the access control that makes the major building block of any system's security. User identification/authentication has been traditionally based on:

* something that the user *knows* (typically a PIN, a password or a passphrase) or

* something that the user *has* (e.g., a key, a token, a magnetic or smart card, a badge, a passport).

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35612-9_23

B. Jerman-Blaži et al. (eds.), *Advanced Communications and Multimedia Security*

These traditional methods of the user authentication unfortunately do not authenticate the *user* as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Biometrics, on the other hand, authenticate humans as such – in case the biometric system used is working properly and reliably, which is not so easy to achieve. Biometrics are automated methods of identity verification or identification based on the principle of measurable physiological or behavioural characteristics such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are (or rather should be) unique and not duplicable or transferable. While the advantages of biometric authentication definitely look very attractive, there are also many problems with biometric authentication that one should be aware of.

2. THE LAYER MODEL

Although the use of each biometric technology has its own specific issues, the basic operation of any biometric system is very similar. The separation of actions can lead to identifying critical issues and to improving security of the overall process of biometric authentication. The layer model was designed by our biometrics team (the authors, Hans-Peter Frei, Kan Zhang) during the Ubilab biometrics project, and its structure is also similar to some findings presented in other seminal works on biometric authentication (e.g., [3, 5]).

The whole process starts with the enrolment:

2.1 First measurement (acquisition)

This is the first contact of the user with the biometric system. The user's biometric sample is obtained using an input device. Quality of the first biometric sample is crucial for further authentications of this user. It may happen that even multiple acquisitions do not generate biometric samples with sufficient quality. Such a user cannot be registered with the system. There are also mute people, people without fingers or with injured eyes. Both these categories create a 'fail to enrol' (FTE) group of users. Users very often do not have any previous experience with the kind of the biometric system they are being registered with, so the first measurement should be guided by a professional who explains the use of the biometric reader.

2.2 Creation of master characteristics

The biometric measurements are processed after the acquisition. The number of biometric samples necessary for further processing is based on the nature of given biometric technology. Sometimes a single sample is sufficient, but often multiple (usually 3 or 5) biometric samples are required. The biometric characteristics are most commonly neither compared nor stored in the raw format (say as a bitmap).

2.3 Storage of master characteristics

After processing the first biometric sample(s) and extracting the features, we have to store (and maintain) the newly obtained master template. Choosing proper discriminating characteristic for the categorisation of records in large databases can improve identification (search) tasks later on. There are basically 4 possibilities where to store the template: in a card, in the central database on a server, on a workstation or directly in an authentication terminal. The storage in an authentication terminal cannot be used for large-scale systems, in such a case only the first two possibilities are applicable. If privacy issues need to be considered then the storage on a card (magnetic stripe, smart or 2D bar) has an advantage, because in this case no biometric data must be stored (and potentially misused) in a central database.

As soon as the user is enrolled, she can use the system for successful authentications or identifications. This process is typically fully automated and takes the following steps:

2.4 Acquisition(s)

Current biometric measurements must be obtained for the system to be able to make comparison with the master template. These subsequent acquisitions of the user's biometric measurements are done at various places where authentication of the user is required. It is often up to the reader to check that the measurements obtained really belong to a live persons (the liveness property). In many biometric techniques (e.g., fingerprinting) the further processing trusts the biometric hardware to check the liveness of the person and provide genuine biometric measurements only. Some other systems (like the face recognition) check the user's liveness in software (time-phased sampling).

2.5 Creation of new characteristics

The biometric measurements obtained in the previous step are processed and new characteristics are created. Only a single biometric sample is usually available. This might mean that the number or quality of extracted features is lower than at the time of enrolment.

2.6 Comparison

Currently computed characteristics are compared with the characteristics obtained during enrolment. If the system performs (identity) verification then these newly obtained characteristics are compared only to the master template. For an identification request the new characteristics are matched against a large number of master templates.

2.7 Decision

The final step in the verification process is the yes/no decision based on a threshold. This security threshold is either a parameter of the matching process or the resulting score is compared with the threshold value. Although the error rates quoted by manufactures (typical values of equal error rate (ERR)[1] do not exceed 1%) might indicate that biometric systems are very accurate, the reality is much worse. Especially the false rejection rate is quite high (very often over 10%) in real applications. This prevents legitimate users to gain their access rights and stands for a significant problem of biometric systems.

3. WHAT ARE THE ADVANTAGES OF BIOMETRIC AUTHENTICATION

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they *authenticate the user*. These methods use real human physiological or behavioural characteristics to authenticate users. These biometric characteristics are (more or less) permanent and not changeable. It is also not easy (although in some cases not principally impossible) to change one's fingerprint, iris or other biometric characteristics.

Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords.

Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication, yet biometric characteristics can be stolen from computer systems and networks. Biometric characteristics are not secret and therefore the availability of a user's fingerprint or iris pattern does not break security the same way as availability of the user's password. Even the use of dead or artificial biometric characteristics should not let the attacker in.

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.