World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:1, No:6, 2007

Biometrics Authorize Me!

João Nóbrega Brites Moita

***Abstract*—**Can biometrics do what everyone is expecting it will? And more importantly, should it be doing it? Biometrics is the buzzword "on the mouth" of everyone, who are trying to use this technology in a variety of applications. But all this "hype" about biometrics can be dangerous without a careful evaluation of the real needs of each application. In this paper I'll try to focus on the dangers of using the right technology at the right time in the wrong place.

***Keywords*—**Authentication, Authorization, Biometrics.

I. Introduction

ACCORDING to Gartner Group, all new "hot" technologies go through a set hype cycle, although at different paces. After an initial breakthrough has occurred, unrealistic projections arise. This is when the technology does not live up to all the inflated expectations created around it. Only after this stage, when a true understanding of the capabilities of the technology has been acquired, can the real benefits of the new trend be implemented with some success [1].

"Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic" [2].

Authentication is the process of confirming a person's identity either by verification (one-to-one comparison to confirm a claimed identity – Am I who I claimed I am?) or by identification (one-to-many comparison in order to establish the identity of a subject from a set of enrolled individuals – Who am I?). Authentication methods can be divided into three categories:

Something you have – such as smart card, USB token, passport, etc.
Something you know – such as a password or a PIN
Something you are – biometrics

Although biometrics has some advantages when compared to other authentication technologies, in that it cannot be misplaced or forgotten, it alone does not solve the authentication problem, and in fact raises some new issues that must be taken into consideration. However, when combined with other methods of authentication in order to implement a two-way or even a three-way authentication factor, it is a very powerful tool.

Any human physiological or behavioral characteristic can be used in a biometric system, provided that it meets the following requirements: universality, uniqueness, permanence, collectability, performance, acceptability, circumvention [3]. The main problem when it comes to biometric technology is where to store the user's template. It is unanimously accepted that the integrity of the biometric data is of utmost importance, so that it is impossible for the data submitted on the enrolment process to be changed, even by the user.

In order to solve this problem, it is common to combine both biometric, smart-card and PKI technologies. Storing the biometric template on a smart card increases protection against attacks and enhances individual privacy, since each user controls his/her own card. On the other hand, PKI uses public key cryptography for user identification and authentication. Despite the fact that it is mathematically more secure than biometrics, the main drawback is the management of the private key. To be secure, the private key must be protected from compromise, but it also needs to be portable in order to be useful. The solution is often to store the private key on a smart card and protect it with biometrics. Thus, this hybrid technology approach uses the smart card as a tamper-resistant module for storing a private key that will authenticate the user on some system by using PKI. Access to the private key should be controlled by some biometric method. This means that if a user wishes to be authenticated, even though the system may only need PKI, in fact a 3-way factor authentication is being used: *something I know* – the private key; *something I am* – the biometric authentication as an control mechanism to gain access to the private key; *something I have* – the smart card.

II. Authentication and Authorization

These two concepts are sometimes misunderstood. It is not hard to make some confusion between an authentication mechanism and an authorization mechanism. The reason for this is because in most host-based systems, and even in some server-based systems, they are performed by the same hardware and sometimes even by the same software [4]. Despite the fact that both mechanisms are tightly-coupled – it doesn't really makes sense to talk about authorization if an authentication mechanism didn't took place before – the truth is that the two mechanisms are totally different, in terms of what they are trying to achieve and how they do it.

An authentication service assures that the communicating entity is the one that it claims to be. When dealing with

Manuscript received May 20, 2005.

J. B. Moita was with Royal Holloway, University of London, Egham UK. He is now with Siemens, Rua Irmãos Siemens – Lisbon, Portugal (e-mail: joao.moita@gmail.com).

messages, it assures the receiver that the message comes from the supposed source. There are several degrees of security when it comes to authentication, from plain-text password challenging systems to systems using Kerberos. The common denominator in all systems is the dependency on some unique bit of information which is shared only between the authentication system and the user being authenticated.

Authorization on the other hand is a mechanism that helps a system decide the access level to some resource by a particular authenticated user. Authorization systems provide answers to the questions *"Is user X authorized to access resource R?"*, *"Is user X authorized to perform operation P?"* and *"Is user X authorized to perform operation P on resource R?"* [4].

So, where does biometric stands? Well, most of the people perceive biometrics as a pure authentication mechanism, a more secure way of authenticating users. The questions answered by an authentication system are *"Who is the user?"* and *"Is the user really who he/she claims to be?"*. Apart from biometrics, there's no technology today that really answers to both these questions. When someone provide a username and a password to an authentication system, even if they match with the ones stored, the system cannot be 100% sure that the user who entered the username / password data is the one who he/she claims to be. All the system can be assured of is that someone entered a piece of data that matched the data known to the system. Whether that data was entered by a registered user or by someone to whom the registered user disclosed the information or by someone who illegally got access to that data remains to be verified. In this sense, biometrics does provide an extra level of security. With biometrics, and due to its uniqueness characteristic, an authentication mechanism can now verify if a user really is who he / she claims to be. The Biometric Consortium [5] says in their website that the use of biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the use of passwords or PINs that can be easily forgotten). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

However, it is also my belief that an authentication mechanism should do more than that, it should also provide answers to the question *"If the secret data the user shares with the system gets compromised, is there a way to revoke the old data and register again some new data?"*. We need to have something in mind: there is no such thing as a 100% secure system. Theoretically we could build a system like this, but in 99,9% of the cases, the amount of money spent on a system like that, far exceeds the value of the information it holds. It is true that we are working everyday to make systems more secure with less money, and new technologies emerge every year that allows us to do so. But this is a two-sided question, it's true for us, but it's also true for malicious users, and for a number of reasons that have nothing to do with technology but more with compatibility of software and business processes, it's often the case where hackers are one step ahead.

What I'm trying to point here is that all systems are vulnerable (some more than others…) and sooner or later systems will be attacked and information might leak. If that information happens to be the authentication data of a user, then we have a problem and to prevent an attacker to access other information using a legitimate account we have to disable that account and revoke the authentication data. Now, suppose that the authentication is performed through the use of fingerprint recognition system, how do you deal with revocation? Sure, you can enroll into the system with another finger, but is that practical? Most of the times you will have to enroll two fingers into the system (in case something happens with one of your fingers), which means that in case of revocation, you will only have four more re-enrollments left. After that you better change your authentication systems otherwise someone will have the same access to your systems as your own employees.

III. Biometrics and Authorization

Of course this doesn't mean biometrics is useless. It isn't. Biometrics is a wonderful and powerful technology when used properly. The problem in using biometrics in an authentication system is that it makes use of public data where private data should have been used. As I said before, authentication systems rely on secret data being shared only between a user and the system. If we replace passwords by fingerprints, we are in fact replacing private information – the password (with all the problems associated with it) – by public data – the fingerprint. Fingerprints are everywhere. We left fingerprint traces while picking up a glass, on the mouse of the computer, in our monitor, Portuguese ID cards even have a fingerprint stamped on it. As you can see, that's not exactly confidential information. It's unique and intrinsic to each one of us, but that doesn't make it confidential. Gummy fingers [6] were base precisely on fingerprints left on some plastic material, and with that a finger made of gelatin was able to fool some biometric systems. One may say that the "gummy finger" attack doesn't apply nowadays, as more sensors now detects for the presence of live fingers. However, it is only a matter of time (and money!) until someone comes up with an idea to fool these systems as well. So, where should biometrics be used? As I see it, biometrics makes more sense when used as an access control mechanism, or perhaps I should say as part of an access control mechanism, since biometrics should be only the starting point of an authorization service. As I said before, an authorization mechanism verifies if a user X can perform an operation P on a resource R, and assumes the user X was successfully authenticated by some other mechanism. But it also assumes that the user X is who he / she claims to be when in most cases it shouldn't do that, because it simply can't. So, since authorization and authentication mechanisms are already tightly-coupled, why not transfer part of the

authentication responsibilities to the authorization system? The idea is to have the authentication mechanism answering the question *"who is the user"* to validate a user's credentials and then the authorization system, before performing a yes or no decision regarding the access to a particular resource, and only at that time, to verify if the user is in fact who he / she says. This is basically a two-factor authentication system but in this case the verification of each factor is performed independently and at a different time, with different goals and perhaps by different systems. This would put biometrics as part of the authorization process, despite the fact that what it does is in fact a second authentication of the user.

IV. Conclusion

In a nutshell, the idea explained in this paper is to use biometrics as part of the authorization mechanism instead of in the authentication mechanism. It would still authenticate a user but in a different way. Instead of performing the authentication when a user enters a system and then perform the authorization mechanism every time the user accesses a resource, the idea is to split the authentication process in two different parts. In the first part the user should present some sort of private information to the system. If successfully authenticated the user can now access the resources the system holds. However, before accessing those resources, the authorization mechanism should decide if the user's credentials presented in the first part of the authentication mechanism are valid for the user to perform the requested operation. In order to make a decision, the system should be certain that the credentials were presented by the user to whom the credentials really belong to. This is where biometrics should be used, to perform a second authentication but now without the need for confidential information; all the system needs to verify now is the authenticity of the user. Why? Well, first of all because the user is identified already (through the use of a username / password for example), hence all we have to do now is to make sure that the credentials presented to the authentication systems were in fact presented by the real user and not by someone else. This gives us more flexibility, in the sense that we are now able to use public information to validate the user. Note that public information doesn't mean insecure information. The fact that fingerprints' data is public doesn't mean it shouldn't be protected. Fingerprint templates should be seen as the public key in a PKI system. The key is public, everybody is allowed to see it (although not exactly encouraged to…) but measures should be taken regarding the integrity of the public key. Everybody can see it, but no one, not even its owner, should be able to change it.

Remember that a biometric characteristic is unique and intrinsic to each one of us. And if this is good for obvious reasons, it also gives you just one "password" for your entire life. If that "password" gets compromised, then you have a serious problem in hands… literally!

References

[1] *Mobile eBusiness*, *Magic Software Enterprises whitepaper*, 2000
[2] An Introduction to biometrics, http://www.biometrics.org/html/introduction.html
[3] A. Jain, R. Bolle, S. Pankanti, "Biometrics – Personal Identification in Networked Society," *Kluwer Academic Publishers*, 2002
[4] Authentication Vs. Authorization, http://www.oit.duke.edu/~rob/kerberos/authvauth.html
[5] The Biometric Consortium, http://www.biometrics.org
[6] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint System," *Prepared for proceedings of SPIE vol#4677*, January 2002