BIOVAULT®: Using Biometrics in Electronic Commerce.

B.L. Tait

Prof. SH Von Solms

RAU – Standard Bank Academy for Information Technology

bt@adam.rau.ac.za

basie@rkw.rau.ac.za

011- 489-3241

Abstract

Currently institutions apply biometrics in the corporate world mainly for access control, and more specific, physical access control.

However biometrics presents the environment with a lot more than just access control. This technology is currently the only technology that can link the user and his authentication token/feature directly. If we consider tokens like smartcards, passwords or special keys, we know that an electronic environment can only authenticate the authenticity of the presented token and not the user presenting this token.

In the world of electronic commerce we need a system that can enforce identification, authentication and non-repudiation with a very high level of certainty, before the services of authorization and privacy can be successfully implemented.

Biometrics gives us two of these security services, making a huge difference in the possibilities of electronic trade and transactions.

In this paper we will explore the possibilities of biometrics as part of a electronic commerce system, with specific consideration to

- *biometric feature safety during network transmission,*
- *the pitfalls of using a biometric feature over an open network*[1] *medium like the Ethernet protocol,*
- *the advantages if a biometric feature can be used securely (without the possibility of compromising the feature) to identify and authenticate the user,*
- *Exploring the possibilities of identifying fraud during the course of a transaction.*

Introduction

There is very little doubt that Biometrics will be part of the very immediate future. After the September 11 attack, the demand for biometrics increased in many areas of identifying people, of which airports saw the immediate benefit, and started installing iris biometric systems at terminals. [1]

We have always used some form of biometrics for identification and authentication [2]. People in a small town would identify and authenticate each other when speaking on the phone (voice biometrics) or when a person would come into a shop (facial biometrics). All of this was done without using computers because people knew each other.

[1] Nearly all the networks we work on today is an Open network (Ethernet and Internet for instance share a common communication medium for network traffic.)

The challenge today is to identify and authenticate a person using computer assistance [2]. We must benefit from the new technologies that allow a computer to recognize patterns with a high level of certainty, and utilize the speed that a computer can do this.

Currently we see a huge rise in access control applications for biometrics. People will be allowed access to restricted areas if their biometric feature checked out with the feature stored in the database.

In this paper we will go beyond physical access control and propose an approach to use biometrics in the electronic commerce environment.

Some background

The question remains: Why biometrics is not currently used for electronic trade?
From time to time someone proposes the combination of Biometrics and Smartcards or Javacards [2], but for one or other reason this never caught on very widely. Maybe one reason might be the fact that we are already using a biometric feature with a credit card (a signature is some form of a biometric feature, with the difference that the user must compare the master signature on the back of the card, with the signature presented by the accountholder). People feel that the additional cost for adding more sophisticated biometric equipment is not worth the means [5].

One major problem the electronic commerce environment faces is the potential identification and authentication of users all over the world. In many cases, fraud takes place because passwords are not used properly. Very few IT security experts probably use very strong passwords, but for the rest of the world, people choose rudimentary passwords, that could easily be guessed, or cracked with password software like loptcrack[8]. Furthermore passwords are stolen, intercepted during transmission etc. It is well known that passwords can be the weak link in security.

As for biometrics, the biggest problem with sending and receiving biometric features is the risk of biometric compromise and replay. If a password or token is stolen, the user can change the password, or receive a new token (like a smartcard being re-issued). If a biometric feature is stolen, the user had lost something that can not be replaced. Considering that we only have 10 fingers, (and) 2 irises, this can be a problem. For this reason people do not want to send their biometric feature over the internet or any network, because if it gets stolen, they can not replace it.

In this paper we will address among others, a system (solution) to address the issue of biometric feature replay.

Using Biometrics for e-Commerce

The solution proposed, is based on a registered patent. This solution called BIOVAULT® unites a number of current technologies, and introduces a new way for electronic commerce security.

With the current technologies, a server will never be able to distinguish between a password that is authentic and a password that was replayed. Using a time stamp only allows the server to conclude that a token took long to arrive, but it can not be sure if the password was sniffed and replayed or just late because of network congestion. A password that was accepted today (and compromised) will be accepted in a weeks time, or until the password is changed on the system

There really is no real relationship between a user and his password or token. The only way that current systems function is based on the secrecy of the passwords and ownership of given tokens. If the password is known to more that one party a computer will authenticate both these parties based on the same password.

With the introduction of biometrics, we know that the person physically presenting the biometric feature is the owner of the feature. If a user presents his iris, it must be the authentic iris, and therefore the authentic user. No two persons could share an iris (like the example of sharing a password) to authenticate themselves.

It is really very difficult to physically steal a biometric feature. Depending on the application, different types of biometrics can be used, ranging in varying levels of compromise ability. To date the two biometric systems proving really difficult to compromise is a) Iris Biometric feature, and b) Facial Thermography biometric feature [4].

Introduction of BIOVAULT®

BIOVAULT® is a new approach to the usage of biometrics as an Identification and Authentication mechanism. The underlying protocol of BIOVAULT® is presently being patented by the RAU University. Because of this, the details of this underlying protocol are not provided here, although it is in the process of being tested thoroughly.
BIOVAULT® will change the way that users will enter into electronic commerce transactions.

BIOVAULT ® is based on a protocol similar to the well known private and public key approach. This means that the user will own a public Biometric key, and he will also own a Private Biometric Key.

Capabilities of BIOVAULT®

1) Users will from need their biometric feature to do any electronic transaction. This will include any instance where the user must prove his authenticity for the usage of any transaction related procedure. If a user wants access to his banking details online, the BIOVAULT® system can be used. If the user want to place a bid on E-bay[7], BIOVAULT® can be the system that link the person placing the bid to account that will settle the amount if the bid is won

2) Servers will have the capability to distinguish between an authentic presented biometric token, and a token that was sniffed and replayed – without using timestamps or encryption(This is part of the BIOVAULT® patent). By keeping it simple, we can prove that a biometric token was sniffed and replayed. The BIOVAULT ® by design allows us to find the non authentic tokens between the authentic ones, and thus prevent any further fraudulent transactions.
3) The problem of submitting any biometric feature over an open network is solved. As already stated, one of the biggest problems with biometrics is sending the biometric token over a open network. Anybody can sniff the messages passing on the open network, and "steal" a persons' biometric feature. With BIOVAULT ® this problem is solved.

<u>Application environment of BIOVAULT®</u>

BIOVAULT® is the underlying technology and protocol for many different application domains to follow.

To follow is a few examples of how BIOVAULT® can be utilized as a underlying technology for different environments:

In store Purchases:

With the introduction of BIOVAULT® it will now be possible to purchase goods directly in a shop without the need for a credit card, smartcard, or any tokens that clutter the purchase process. A User will present his private biometric key, and if this feature matches his public biometric key, the purchase can be approved.

With any in store purchase, the user can only be himself. Thus no person can masquerade as someone else, because your proof of identity is placed in a Biometric feature that you always have with you

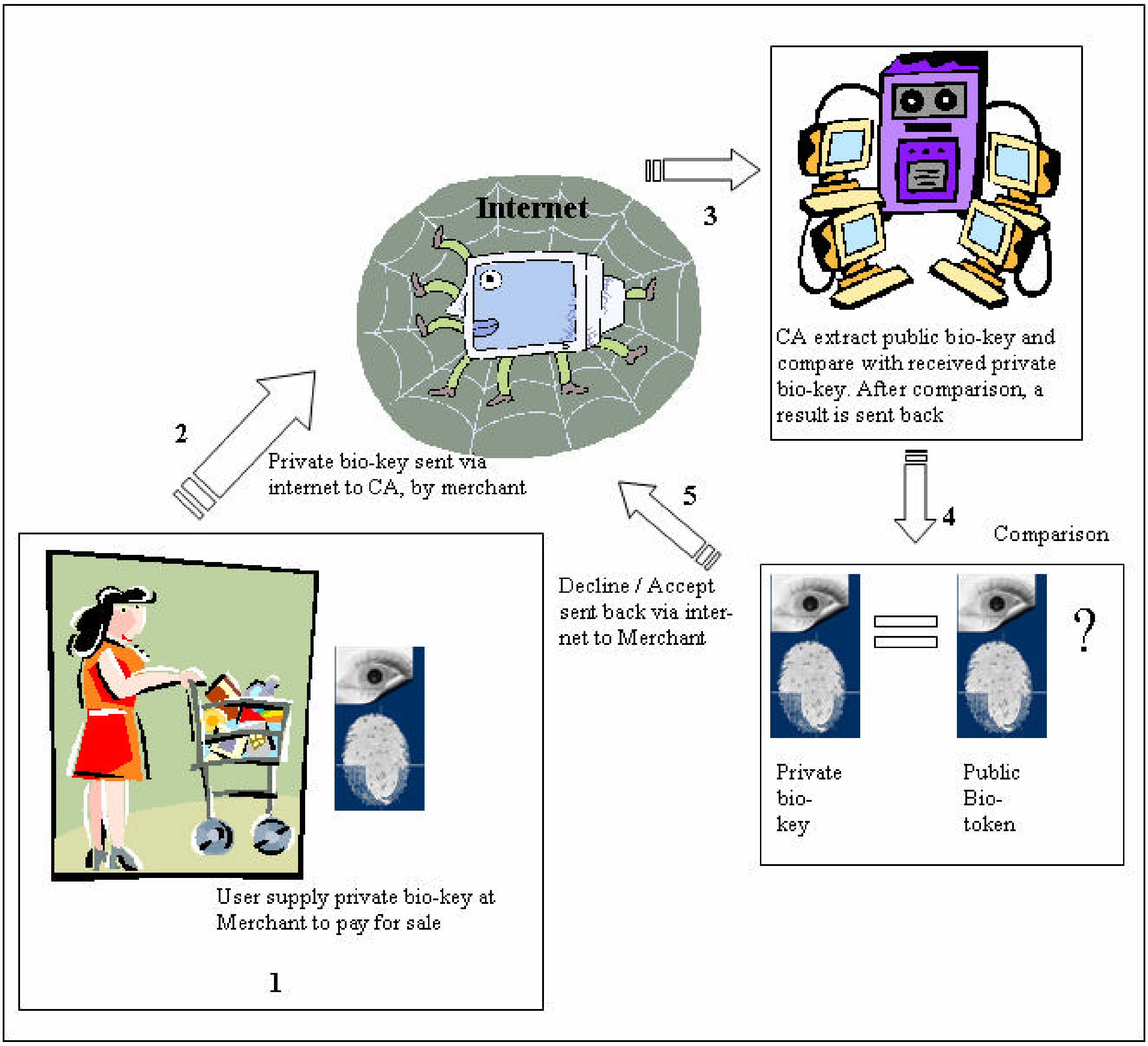
Internet
3
CA extract public bio-key and compare with received private bio-key. After comparison, a result is sent back
2
Private bio-key sent via internet to CA, by merchant
5
4
Comparison
Decline / Accept sent back via inter-net to Merchant
Private bio-key
Public Bio-token
?
User supply private bio-key at Merchant to pay for sale
1

Diagram 1: Example of an in store purchase

Internet purchase

This is where the real power of BIOVAULT® will be apparent. Presently the biggest problem we face as suppliers and as buyers is the possibility that a presented Credit Card is stolen and used fraudulently.

All current technologies like Paypal [6] rely on the fact that a user will keep his password safe and secret, and that only the authentic user will have access to his password.

With the introduction of BIOVAULT® the trading community can be 100% sure that the user presenting his private biometric key is the authentic user. If the user is a hacker that sniffed the biometric token, and replayed it, BIOVAULT ® will pick this anomaly up.

All internet transactions will benefit in a big way with the usage of BIOVAULT®, even placing a bid on E-bay [7] or any auction site where authenticity is very important.

Sending of BIOVUALT® signed messages.

Another direct advantage of BIOVUALT® is the capability of sending a true digitally signed message.

A user of the BIOVAULT ® system will be able to send a e-mail or any electronic message and sign the message with his/her BIOVAULT feature. The user on the other end will then be able to check the authenticity of the message, and be 100% sure that the message actually came from the authentic sender.

BIOVAULT® and supporting technologies.

Currently biometrics will only provide us with the security services of Identification and Authentication.

A proper PKI environment will allow for the rest of the security services, namely Non-repudiation, Authorization and Confidentiality.

BIOVAULT ® by design is part of a public private key environment, but with the difference that the keys are replaced with biometric features.

This means that by using BIOVAUL®, we satisfy all 5 security services with one system.

Conclusion

Electronic commerce will only be really secure the day that Biometrics become part of the environment. We can not deny this.

However, we need a solution for the problems we are presently facing with the use of biometrics. These problems include stealing a biometric feature, replaying of a biometric feature, and using biometrics for more than just Identification and authentication.

We are confident that BIOVAULT® solves most, if not all of these problems.

Recognition: The research reported in this paper is done with a grant from the National Research Foundation (NRF)

References

[1] Secrets and Lies – Digital security in a Networked World. Bruce Schneier.

[2] Biometriese enkel aantekening tot IT stelsesl B.L. Tait

[3] Namitech – http://www.namitech.co.za

[4] Biometics – A look inside. John D. Woodward Jr.

[5] Biometrics: Advanced Identify Verification: The Complete Guide - Julian D. M. Ashbourn

[6] Paypal – http://www.paypal.com

[7] E-bay – http://www.ebay.com

[8] LopthCrack – Http://www.lopt.com