BIOVAULT: SOLVING THE PROBLEM OF REPLAY IN BIOMETRICS

An electronic commerce example

Prof Basie von Solms & Bobby Tait
Johannesburg University

Basie@adam.rau.ac.za, bobby@csrau.rau.ac.za

Abstract: One of the major risks involved in using biometrics for identification and authentication over open public networks, is the danger that the electronic biometric token (for e.g. a fingerprint or iris) can be intercepted and replayed by an unauthorized party. Furthermore, it is possible to make an unauthorized copy of a biometric token, without the permission and knowledge of the real owner, and use that for unauthorized transactions. This can for e.g. happen when a fingerprint is 'lifted' from an object the owner has used, and a latex copy is made from this token [5].This paper reports on a system in development, called Biovault, which addresses precisely the problems mentioned above, and which may help to make biometric tokens much safer to use over open public networks, for specific application in electronic commerce.

Key words: Electronic Commerce, Biometrics, Biometric Tokens, Identification, Authentication, Replay, Identity theft

1. INTRODUCTION

Identification and authentication over insecure networks had always been a problem that caused serious information security risks. Several reasons for this can be identified, but the two discussed below are amongst the most serious ones.

Firstly, a password, even in encrypted form, can be intercepted by a third party, and reused or replayed at a later stage without the knowledge of the owner of the password.

The system which performs the authentication will never know whether the password is the original version originating from the real owner, or whether it is a replayed version of the password [4].

Supporting technologies like time stamps may help, but do not solve the problem completely.

Digital Identities, allowing the use of digital signatures, do offer some help, but do also not solve the problem, as there is no real relationship between the user and his digital identity.

Secondly, with both passwords and digital signatures, the real owner is not authenticated – rather the person who is in possession of the password or private key needed to create the digital signature, is authenticated [1]. If the password or private key had been compromised in any way, unauthorized people may masquerade as the real owner, and the computer system will not be able to identify this masquerading. The bottom line is that the system doing the authentication cannot determine whether the real owner, or a masquerader, is offering the password, token or digital signature.

Biometrics, of course, goes a long way in solving the second problem discussed above [2]. In most cases, the real owner of the biometric token must be present when the token is 'taken', for e.g. when a fingerprint is scanned on a digital fingerprint reader. Therefore the token is directly linked to the owner, and cannot be used by someone else [4].

Again, this is however not always true. A biometric token can be 'lifted' from an object handled by some person, and techniques do exist to make a copy of that lifted token and use it in a replay situation [5].

Furthermore, even when using biometric tokens, the same risks as for passwords exist. A biometric token send over an insecure network can be intercepted, and replayed at a later stage, without the knowledge and authorization of the real owner.

As in the case of the password, the computer system will not know whether the token is supplied by the real owner, or by a masquerading person.

The problems discussed above are some of the major reasons why biometrics had not yet moved into the mainstream for identification and authentication over insecure networks.

The system described in this paper, Biovault, goes a long way in addressing the problems identified above.

In the following paragraphs, we will describe how Biovault does address these problems, and what future research and development are envisaged to use Biovault as a secure biometrically based identification and authentication mechanism for e-commerce over insecure networks.

2. THE BASIS OF BIOVAULT

The basic design pillar, on which Biovault is based, has to do with what we call the symmetry and asymmetry differences between password and biometric tokens.

2.1 Symmetry

When an offered password is matched by a computer system to a stored version of the specific password, a 100% match is required, i.e. the offered version must exactly match the stored version – we call this symmetric matching because the error acceptance ratio between the 2 versions must be zero to accept the offered version as valid.

2.2 Asymmetry

When an offered biometric token is matched by a computer system to a stored version of the specific biometric token, a 100% match is not required – actually the chances of a 100% match is anyway very slim. This is inherent in the mathematical algorithms used to create and match biometric tokens. The algorithms must make provision for the fact that, for e.g. a fingerprint, can be positioned a little differently on the reader as when the stored master copy was read. The error acceptance ratio between the offered and stored versions is therefore greater than zero – the precise ratio can be set, and any offered token differing form the stored version within the error acceptance ratio, will be accepted as a match, and therefore lead to valid authentication. For this reason we call this asymmetric matching

2.3 The Token Archive (TA)

Biovault makes use of the fact that if an offered biometric token and any stored biometric token matches 100%, the chances that the offered biometric token is a replay of a previously used biometric token, is very high, and the offered biometric token is not accepted.

For this model to function a Token Archive (TA) is introduced on the Authentication Server. This TA will store all biometric tokens that the user ever used in his life time. It is quite clear that this TA might become very big, hence take long to search and match the offered token with the whole TA.

In order to speed up the searching of possible 100% matches in the TA, all biometric tokens will be sorted ascending in the TA, making it possible to do binary searching inside the TA. Using Binary Searching will allow the server to detect a possible 100% match at incredible speeds. The matching speed is described by the function O(LogN) [6]. This function demonstrates that as data becomes larger, there is no significant rise in search time

The following paragraph describes the first (initial) version of Biovault.

3. BIOVAULT VERSION 1

This initial version made provision for a Biovault master copy of the owner's biometric token stored during the registration phase, as well as a Biovault Token Archive (TA) stored on the computer system.

Whenever a token is offered to the computer system, the offered token is first compared with the Biovault master copy of the token stored during registration of the user. If a non-identical match within the acceptance ratio is determined, the offered token is then compared with all versions stored in the TA. If an identical match is found with any version stored in the TA, the offered version is rejected, and the user is requested to offer another copy. The process is then repeated with the new offered copy received.

If no identical match is found between the offered copy and any version stored in the TA, the offered version is stored in the TA, and the offered version is accepted as a valid token, and the user is authenticated.

Figures 1 illustrates this operation

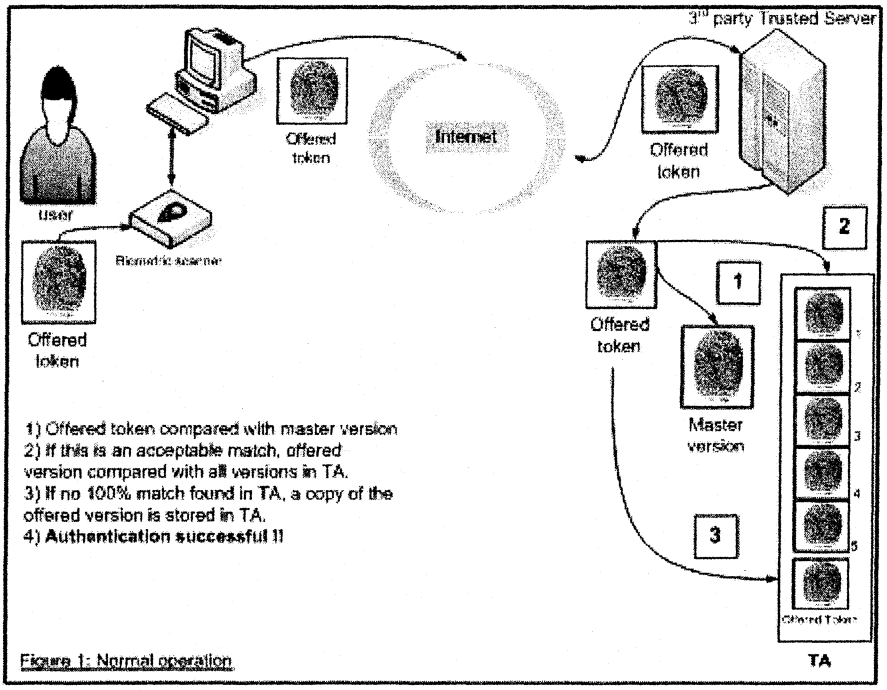

Figure 1. Normal Operation

If the offered token was intercepted while being sent to the computer system, this intercepted version could be replayed at a later stage to try to masquerade as the real owner.

Biovault Version 1 however, recognizes this replay attempt. When the replayed version was received by the computer system, it was first compared to the stored master version. If an acceptable match was found, it was compared to all versions stored in the TA. In this case a 100% would be found, because the original offered version, of which a copy was intercepted, had been stored in the TA. The replayed version would then be rejected.

This is illustrated in Figure 2.

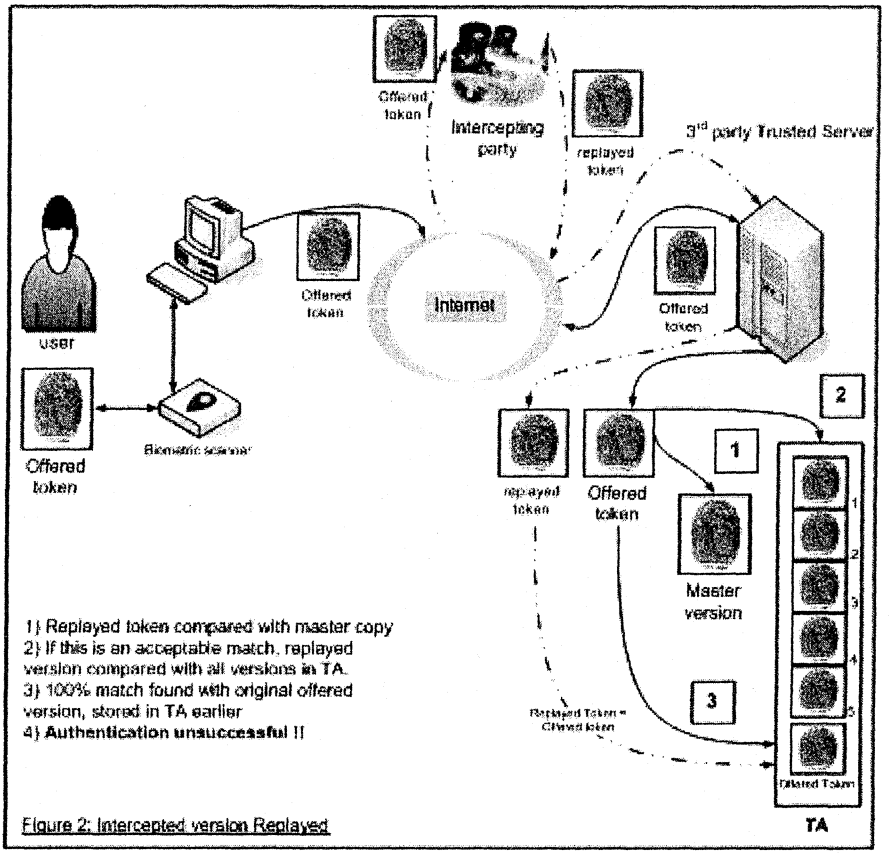

Figure 2. Intercepted version Replayed

The developed system works perfectly. It was proved easily that if an offered token is intercepted during a transaction, and the interception does not cause the aborting or termination of the transaction – ie the offered token does reach the computer system, replay of the intercepted token at a later stage, results in the replayed token being recognized as such and rejected.

The concept of the TA therefore seemed to solve some of the major problems.

However, some other problems still could not be solved.

Firstly, if a unauthorized token, 'lifted' from some object is replayed into the system, Biovault Version 1 accepted the lifted version, because it did not have an identical copy of the lifted version in its TA, and therefore assumed this version to be 'unblemished'. Biovault Version 1 could not determine whether this version really came from the real owner – all it could determine

is that it had not received this version of the token before. This is illustrated in Figure 3.

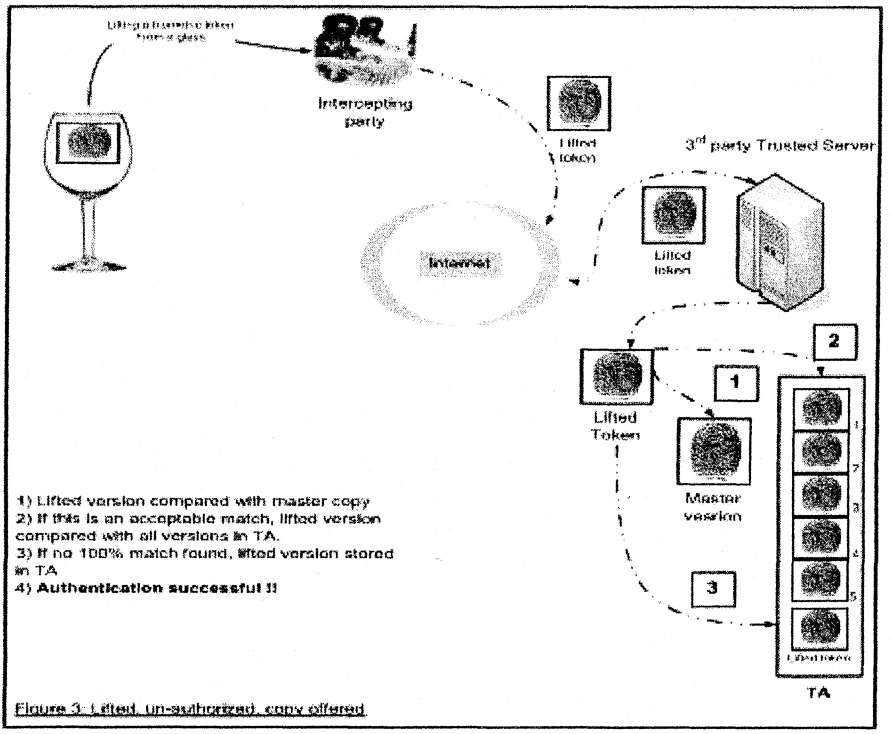

*Figure 3.*Lifted, un-authorized, copy offered

Secondly, it was determined that if a (clear text) token is intercepted, it is possible to 'tweak' the electronic version of the intercepted token in such a way that it differs from the original version just enough to be accepted by the computer system. The tweaking resulted in another version of the original token, differing just enough to still fall within the error acceptance ratio.

Biovault Version 2 addressed both problems by using encryption.

4. BIOVAULT VERSION 2

This version ensured that the offered version, ie the one acquired directly from the owner, was first 'digitally signed' by the owner, by encrypting it with the private key of the owner. The computer system then first decrypted the offered version with the public key of the owner. (The reader is assumed to be up to date on the theory of Public Key encryption).

This approach solved both problems identified in Version 1.

Firstly, any 'lifted' version was not digitally signed by the owner, and when decrypted by the computer system using the public key of the owner, always resulted in an electronic string which fell outside the error acceptance ratio, and was therefore always rejected.

Secondly, trying to 'tweak' the digitally signed version of the offered token always resulted in a string which was rejected. Tweaking an encrypted version of the offered token was exceedingly more difficult than tweaking the clear text version.

Note that if a digitally signed version of the offered token was intercepted and replayed, it would immediately be recognized as a reply, because the offered version itself would by that time, be stored in the TA. This is just a more advanced case of the situation described in paragraph 3 above.

Biovault Version 2 worked perfectly, and solved many of the problems inherent in Biovault Version 1.

However, some more problems and difficulties were identified.

Firstly, requiring all participants to have a Public/Private key pair in order to digitally sign biometric tokens, placed a significant burden on potential rollout of Biovault. Furthermore this did not really improve on systems that uses biometrics to gain access to one's private key [7]. All that Biovault 2 accomplished was merely to use ones private key to gain access to your biometric token.

Secondly, we were still worried that a token, digitally signed by the owner, could be intercepted, and the transaction in some way aborted or terminated before the offered token reached the computer system. If this happened, the offered token would not become part of the TA (because the computer system never received it), and the intercepted version could then successfully be replayed at a later stage. This is illustrated in Figure 4.

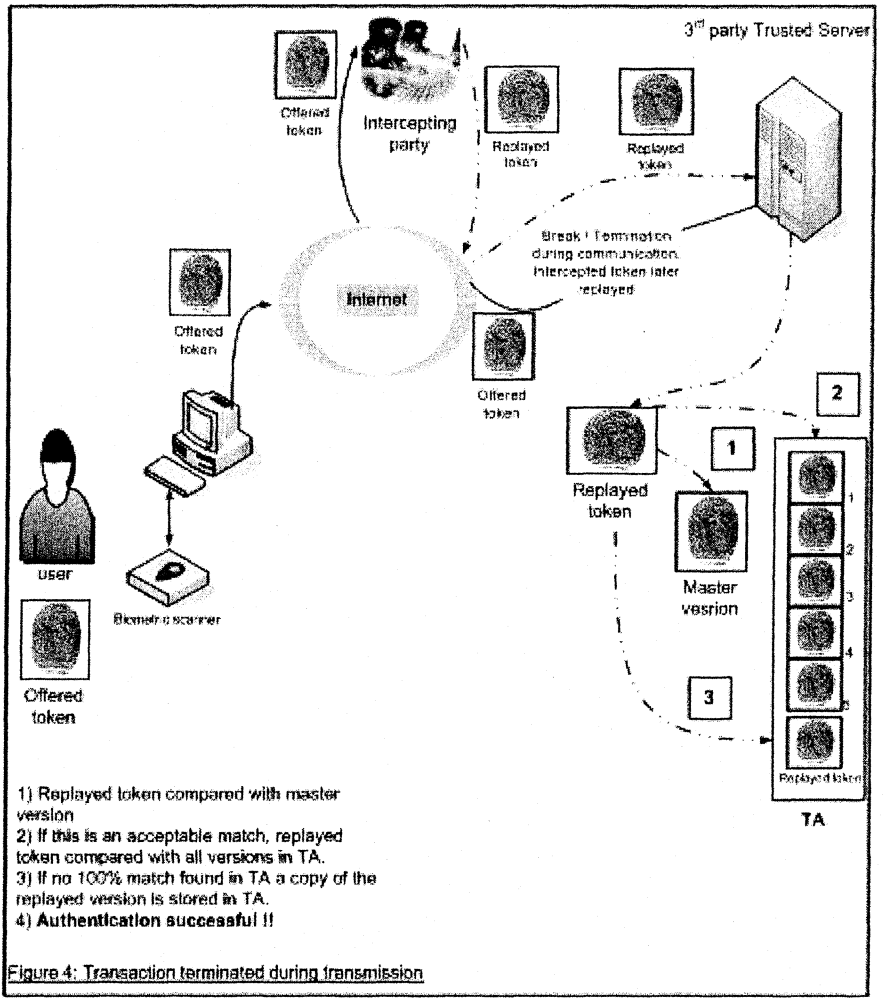

Figure 4. Transaction terminated during transmission

This resulted in Biovault Version 3

5. BIOVAULT VERSION 3

The inherent problem with Biovault Version 2 was that if a biometric token is created with the involvement of the real owner, ie a token that the owner really wants to offer to the computer system for identification and authentication purposes, the moment this token leaves the workstation of the owner, the owner has no copy or record of that token. If the token successfully reached the computer system, a copy will be stored in the TA.

However, if the offered token is intercepted during transit, and does not reach the computer system, as mentioned at the end of the previous paragraph, neither the owner nor the computer system has a copy. This means there is a 'hot' copy of the offered token, the intercepted version, out in the open. This hot copy can then be used in a replay effort at a later stage. Such an effort will most probably be successful, because the computer system does not have a copy in Biovault master TA.

As an initial option (version 3A) in solving this problem of a hot copy , a personal TA will be created on the workstation of the user, in which a copy of every token sent to the computer system was first stored locally before it was sent to the computer system and offered for identification and authentication.

This meant that no unrecorded 'hot' copies of offered tokens could exist.

By synchronizing the personal and master TA from time to time, it is possible to identify any offered tokens which was sent to the computer system, and never received by the computer system. This synchronizing effort updates the system TA, and caused any offered copy which was intercepted and never reached the computer system, to be included in the master TA. Replaying such an intercepted copy at a later stage, would the result in rejection. The reader should be able to see that this solution solves the problem illustrated in Figure 4. This is illustrated in Figure 5

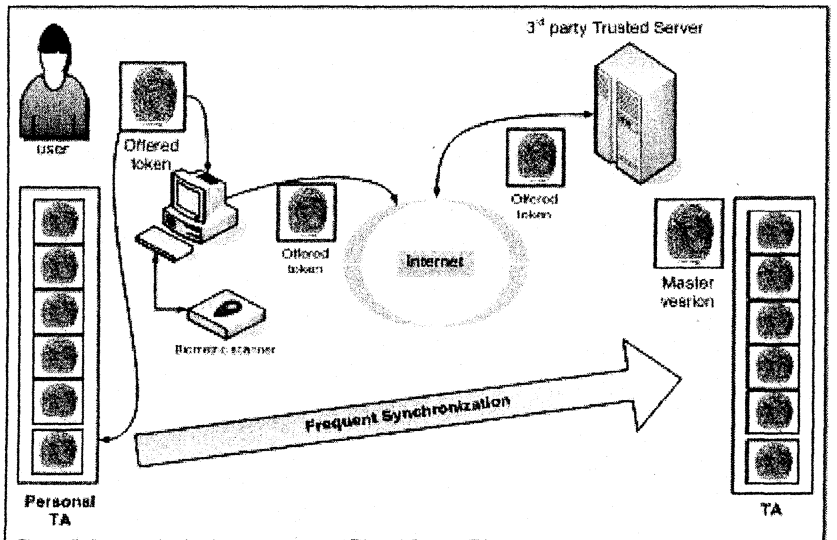

Figure 5: Synchronization between personal TA and System TA

Figure 5. Synchronization between personal TA and System TA

6. A PRACTICAL E-COMMERCE APPLICATION OF BIOVAULT.

One of the primary objectives during the development and research of Biovault was that the developed system must be usable for electronic commerce. Electronic commerce can benefit from an environment where the client can be sure that his money will only be paid from his account on his request. The money vendor like Visa card [8], wants to be sure that the request to pay money, came from a authentic account holder, and a seller like Amazon [9] want to be ensured that they will get their money, and preferably not be informed that the transaction was fraudulent, after goods have been dispatched.

With the development of Biovault, the possibility of biometric replay is not of much concern. In order to demonstrate the usage of Biovault during an online purchase, the process will be discussed in two phases. Figure 6 illustrates the first phase of purchasing a book from Amazon [9]

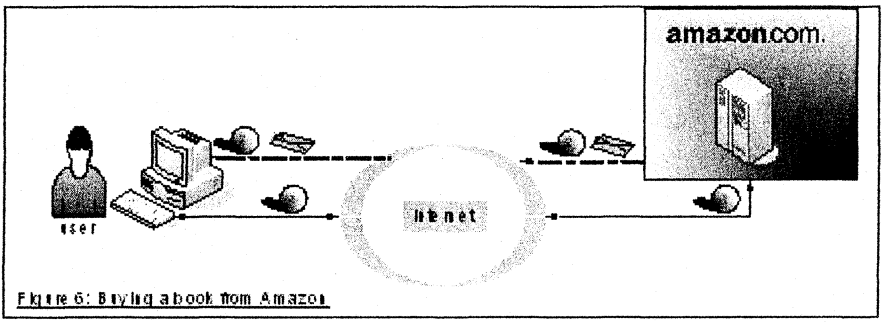

Figure 6. Buying a book from Amazon

During this phase the user will visit the website of Amazon as shown in step 1. The user will then find the book that he wishes to buy, place it in his shopping cart, and proceed to the checkout section on Amazon's website.

Amazon will then inform the user the total amount payable, including shipping and handling, this is illustrated by the little envelope in step 2. This is a familiar process to everybody that buys a book from Amazon. The next phase will demonstrate how the user will use the Biovault model to pay for the book. Currently, when a user uses a token like a credit card to pay for a

transaction, the Visa Card server is contacted by the seller to ensure that the credit card is authentic and that the card is not reported as stolen. Once the authenticity is verified, Visa will inform the seller that the money will be paid, and an authorization code is supplied [8] to the seller. With the Biovault environment the same basic model will be used, and is illustrated in figure 7

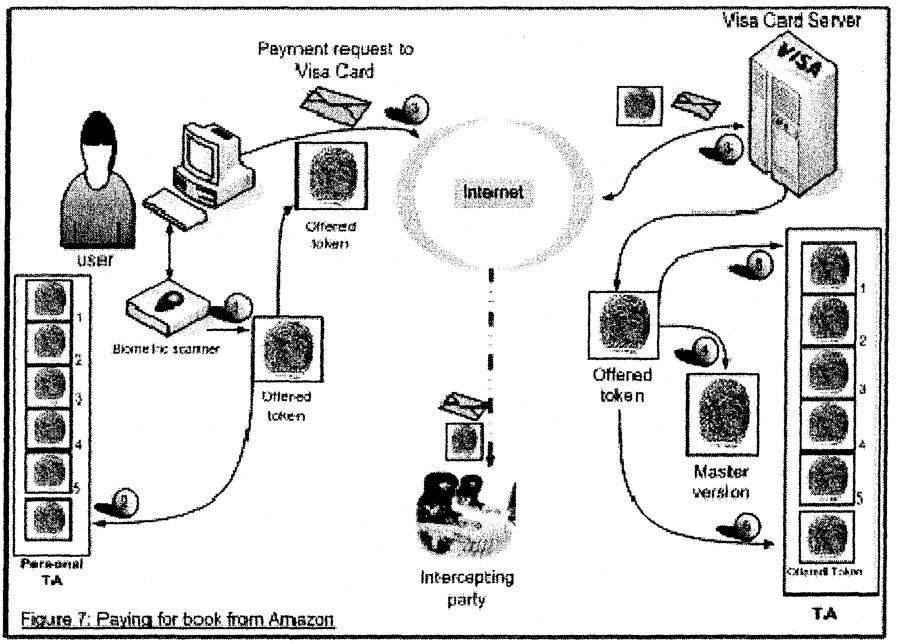

Figure 7. Paying for a book from Amazon

During the first step the user provides a fresh biometric token, this fresh biometric token will be placed in the personal TA during step 2. This will ensure that one keeps track of all biometric tokens destined for payment. The user will then submit the payment request and fresh biometric token to his money vendor, in this example Visa, during step 3.

Take note that the offered biometric token and payment request to Visa is sniffed by an intercepting party during transmission. Step 4 illustrates how the Biovault mechanism authenticates the user against the master version of the biometric token. If the matching algorithm is satisfied with the offered biometric token, the system will proceed to step 5 to confirm weather this offered token is unique and not a replayed old token already in the TA.

If the system did not discover an identical copy in the TA, the new offered token will be added in to the TA in the last step.

At this stage the Visa server is satisfied that it is the authentic user that is requesting money to be paid to Amazon. The Visa server will typically now confirm that the user has the necessary funds available to pay for the Amazon transaction.

If the funds are available, the Visa server will provide Amazon with an authentication code (step 2), for the amount payable. The user will receive a transaction result directly from the Visa Server in step 3. This is illustrated in Figure 8.

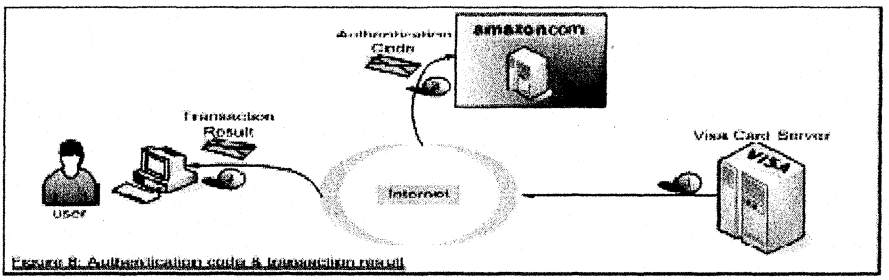

Figure 8. Authentication code & transaction result

7. REPLAY OF INTERCEPTED BIOMETRIC TOKEN.

In order to complete the electronic commerce example, figure 9 illustrates the scenario of a hacker replaying the sniffed biometric token procured earlier in figure 7.

The intercepting party would typically alter the payment request for Visa in such a way that the money must be paid to a Swiss bank account, this results in an updated payment request. The intercepting party will then submit the replayed biometric token and updated payment request to the Visa server indicated by step 1, figure 9.

The Visa server will receive the payment request and biometric token (step 2 in figure 9) and match the replayed token to the master version (step 3 in figure 9). If the matching algorithm is satisfied with the matching ratio, the replayed version will be compared to all the old biometric tokens in the TA (step 4 in figure 9). Step 5 in figure 9 indicates that the token supplied is a token that has been used at an earlier stage, because a 100% is found with a biometric token in the TA.

For this reason the Authenticity of the user is rejected and the transaction is unsuccessful.

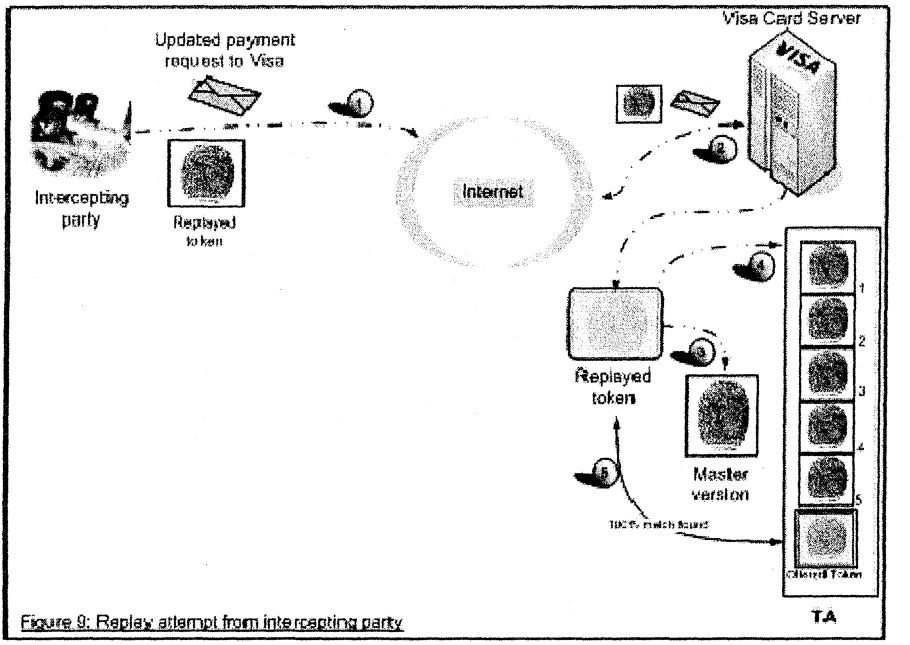

Figure 9. Replay attempt from intercepting party

The reader may reason that in figure 7, if the interception takes place successfully, but the offered token does not reach the Visa card server, a replay of the intercepted token (hot copy), may be successful, because the offered token did not reach the server's TA.

This issue is addressed by the synchronization step illustrated in figure 5, and also extensively addressed in Biovault version 4.

We will not expand on this issue at this point.

8. BIOVAULT VERSION 4

Biovault Version 3 is fully operational. Biovault Version 4 is being designed at present. This version will use Biovault to implement the concept of 'biometric digital signatures'.

Furthermore in version 4 the user will not need to frequently synchronize the personal TA with the server. This version of Biovault will be much easier to roll out, and will not need much additional hardware to function. Version 4 we also address a number of problems still inherent in version 3.

Using this version 4, it is investigated that unique digital signatures can be created using biometric tokens.

9. SUMMARY

We are convinced that Biovault is addressing many, if not all, of the problems which had prevented the very powerful technology of Biometrics to be used properly for identification and authentication over insecure public networks. Biovault allows for applications in many domains, including electronic commerce (as demonstrated), Point of sales transactions, and even Automated teller machine transactions. During the presentation of Biovault, a demonstration of Biovault version 3 will be given as proof of concept.

10. REFERENCES

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

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

[3] Biometrics – A look inside. John D. Woodward Jr. ISBN 0-07-222227-1

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

[5] T. Matsumoto, H. Matsumoto, K Yamada, S. Hoshino, 2002, "Impact of artificial gummy fingers of fingerprint systems" Proceedings of SPIE Vol #4677, Optical security and counterfeit deterrence techniques IV.

[6] http://www.ics.uci.edu/~eppstein/261/f03-outline/11.fraccasc

[7] http://www.activcard.com

[8] http://www.Visacard.com

[9] http://www.amazon.com