A Remote Biometric Authentication Protocol for Online Banking

Anongporn Salaiwarakul
Department of Computer Science and Information Technology, Naresuan University, Thailand
Email: anongporns@nu.ac.th

***Abstract*—This paper presents a remote biometric authentication protocol illustrated by online banking situation. The protocol assures three properties which are crucial if the biometric data is involved in the authentication process. Even if the biometric data is excellent in authenticating the users because it verifies the users by mean of their personal attributes, the biometric data is sensitive in security prospective because it is hard to be kept secret. The biometric authentication works well in supervised situation if the verifier can prove that the biometric data comes from the live presentation of the user at the time of user's verification. Prone to security risk in the unsupervised situation, especially online transaction, where a captured biometric data can be presented to the system, a biometric authentication in remote situation that guarantees the security level should be proposed. To assure this, the security properties of the protocol should be verified and analysed to promise that the protocol does not manipulate the data with an intruder. This paper verifies and analysed the intended security properties of the proposed protocol. The result of the analysis shows that the protocol preserves the three properties: privacy of the biometric data, liveness, and intentional authentication.**

***Index Terms*—biometric authentication protocol, security property, privacy, liveness**

I. Introduction

A password or other methods proof of identity such as smart card or token can be given away or stolen Therefore, the actual identity of the user could not be confirmed. In contrast to those methods, the biometric data belongs to a particular person. Then, it truly reflects the user's personal characteristics so the data can be used to prove the identity of the user. Even the biometric data has its advantage in term of the authentic user's identity; its security should be considered because of its nature. Biometrics is hard to keep secret and human has a limited number of them. Once they are compromised, they can not be changed, replaced or regenerated as a password or a smart card can.

The security of the biometric authentication method depends on the authenticity of the biometric data. Since the biometric data is in the public domain by its nature. An artificial biometric data, e.g. rubber finger that replicates the real user's fingerprint, can be generated so it can often fool a biometric reader. Liveness detection in biometric reader is largely research. Biometric authentication works well in supervised situations but for high assurance situations, the reader should be attended to or at least observed until we get verifiably strong liveness detection. However, this concern mainly relies on research in hardware. Biometric authentication is much harder in the remote or unattended cases.

Authentication in biometric protocol can be compromised in a number of ways: via an attack on the server storing the biometric code, an interception of the biometric data when read by the biometric reader, or an attack during biometric data transmission. Concerning the attacks as described, this paper presents a secure protocol to enhance security level for a remote biometric authentication. Once the security protocol is proposed, it should be verified to assures the security properties that it promised [1] and [2]. Online banking is employed as an example for illustration the proposed protocol. The protocol guarantees the live presentation of the user on the time of verification, liveness property. The paper attempts to demonstrate a remote biometric authentication that assures the liveness property; therefore we assume that the related risks of the online transaction e.g. key logger or viruses is out of the scope. The protocol also reserves the privacy of the biometric data. In addition, the intended purpose of the authentication from the user is verified to prevent the forged intentional purpose from an intruder.

II. The Protocol

Basically an authentication process is used as a prior step before the user's actual activity can be performed. Therefore, this paper considers that a remote biometric authentication protocol has two major activities: authenticating the user remotely using biometric data, and performing user's activities (requests) e.g. online banking transaction. The former process comprises of two components: user and authentication server whereas the latter process involves the user and the service system.

The proposed remote biometric authentication protocol comprises of three components: the User, the Bank (the service system) and the Biometric Authentication Server. He must be ensured that the biometric reader is sincere. To achieve this, *the User* operates his transactions via the local workstation which has Trusted Platform Module (TPM) [3] and [4] installed. The aim of TPM in this

Manuscript received July 1, 2013; revised September 13, 2013.

doi: 10.12720/ijoee.1.4.279-283

protocol is to verify the correctness and the trustworthiness of the machines the user operates. Upon booting up, the user's workstation and the biometric reader are verified by the TPM. The report of the integrity of the local system is sent to the user. The user decides to continue his activities if he satisfies with the integrity value, the verification data. This can protect the user from presenting his biometric data to the counterfeit biometric reader which has the potential to steal the user's biometric data or manipulate with an attacker. The *Bank*, the second component, is responsible for the bank transaction which is transferring money from user's account to the other account as requested by the user. *The Biometric Authentication Server* performs the biometric matching process. The server has the biometric template storage which is used when the stored biometric code is acquired for matching against presented biometric data. The result of the biometric verification is reported to the user. Once the user wishes to perform online banking transaction, the biometric verification result along with the requested transaction must be presented to the bank.

III. Design Considerations of the Protocol

The protocol involves two major activities: authenticating the user, and banking transaction (transferring money), each of which has different consideration. A user is required to verify his identity in order to access his account. As the authentication process requests the user's biometric data, the liveness of the biometric data must be assured so that the bank is certain that the request comes from the genuine user. For the banking transaction, the message must be verified and guaranteed that the account owner is willing to provide his biometric data for the transaction not other transaction that he is not willing to do so. Hence, the intentional authentication property is verified. Therefore, not only the validity of the biometric verification result is checked but the purpose of the biometric authentication is verified. This assures that the user presents his biometric data for the transferring process not for the other unintended purpose.

In this protocol, nonces are used for checking the freshness of messages received and encryption and decryption are also used for the secrecy of message content. Signed messages are used to confirm the origin of the senders. Table I shows the communication messages among the three components.

The communication messages commence when the user requests transfer transaction from the bank. As a response, the bank looks for the user's authentication, in this case – the biometric authentication is applied. The bank sends a signed message which includes the user name, the biometric authentication request, and the nonce n1. The user forwards this message to the biometric authentication server in order to acquire the user's verification. It triggers the BAS to inquire the user's biometric data; the nonce n2 is included in the replied message. This requested message is signed with the BAS's signature. The user presents his biometric data to the reader. The biometric data is signed by the TPM so that the authenticity of the biometric data can be verified. The encrypted message is composed of user name, the nonce n2 and the signed biometric data with the TPM's signature.

To enhance the security requirement in term of liveness of the biometric data, once the biometric data is submitted to the BAS, the BAS verifies the live presentation of the user by acquiring the user to present verification data. The verification data is a secret data which is known only to him and the BAS. The BAS sends an encrypted message of the request and newly generated nonce n3. As a response, the user presents his biometric data, the verification data and the nonce n3. The message is signed with the TPM's private key. The signed message, together with information the user provided, are enciphered by the BAS's public key. The BAS verifies the message by checking the nonce and the signature. It then validates the authenticity of biometric data. The verification result, the user name and the nonce n1 are signed by the BAS.

Upon receiving the verification result message, the user appends his transfer transaction and sends this message to the bank. The transfer message includes the amount and account he wishes to transfer. The message is encrypted by the public key of the bank. The bank deciphers and verifies the validity of the message. It then checks the matching result. If the result is positive, the bank performs the user's request, transferring the money to his desired account.

TABLE I. The Communication Messages in the Protocol

Communication	Message
User → Bank	uName, amount, acct
Bank → User	$sign_{skBank}$(UName, amount, acct, BioAuthReq, n1)
User → BAS	$sign_{skBank}$(UName, amount, acct, BioAuthReq, n1)
BAS → User	$sign_{skBAS}$(reqBD,n2)
User → BAS	$penc_{pkBAS}$(n2,uName,$sign_{skTPM}$(BD))
BAS → User	$penc_{pkTPM}$(reqVD,n3,$sign_{skBAS}$(reqVD,n3))
User → BAS	$penc_{pkBAS}$(VD,BD,n3),$sign_{skTPM}$(VD,BD,n3))
BAS → User	$sign_{skBAS}$(uName,amount,acct,matchResult,n1)
User → Bank	$penc_{pkTPM}$(uName,amount, $sign_{skBAS}$(uName,amount,acct, matchResult,n1))
Bank → User	Transfered Result

IV. ProVerif Model

This paper verifies the proposed protocol using the Dolev-Yao style adversary [5] in analysing the security goals. This style of adversary is able to read messages over the network and collect in its knowledge set. The attacker can also calculate the attack from its knowledge set. This protocol is verified by ProVerif [6] based on applied pi calculus [7]. It can handle unbounded number of sessions of the protocol, generate attacks based on Dolev-Yao style attackers and manipulate messages communicating among components to find any possible

attacks to the protocol corresponding to the intended security properties.

The proposed protocol promises the three intended properties. To ensure that the protocol provides the appropriate level of security and the properties it affirmed, ProVerif is used as the verification tool to verify and analyse the protocol. The ProVerif models consist of three major processes: BAS process, Workstation process and the Bank Process. The BAS process represents the duties of the BAS. Its main task is to authenticate the user and ensure the live presentation of the biometric data. The workstation process represents the user's activities: presenting the biometric data for the biometric authentication and request transfer transaction to the bank. The U process is responsible to input the user's verification data and user's biometric data to the workstation. The Bank process represents the bank's business. It verifies the biometric authentication result and performs the transfer transaction as requested by the user if the authentication is successful. The ProVerif models of the protocol are described in the following section.

A. Equation and Signature Theory

This is the method that ProVerif uses to solve the messages. From the equational and signature theory, ProVerif also forms messages from the provided theory in order to solve whether an attacker can acquire the information that the *query* commands ask for. It, in turn, returns the verification results. The *checksign* operation is performed in order to verify the signature of the message and the information in the signed message is presented. The signed message is performed through *sign*. The *enc* is used for message encryption. The messages are encrypted by public key cryptography. To decipher a message, *dec* is performed to decipher an encrypted message from the known key. The model of the protocol in ProVerif contains signature and equational theory which generate signed messages and messages encrypted by public key cryptography. This process advises ProVerif how to encipher and decipher a message. The *sign* function is used to sign the message whereas the *pk* function is used to generate the public key. The equation *checksign(sign(x,y),pk(y)) = x.* is represented for verifying the signature of a message from the provided public key of the origin. The equation *equation dec(enc(x,pk(y)),y) = x.* represents the deciphement of the public key encryption message. The functions and equations are modeled in ProVerif as following:

```
fun sign/2.
fun checksign/2.
fun pk/1.
fun dec/2.
fun enc/2.
(* EQUATION *)
equation checksign(sign(x,y),pk(y)) = x.
equation dec(enc(x,pk(y)),y) = x.
```

B. BAS Process

When the BAS process receives the authentication request, the BAS responds the request by sending a signed message of newly generated nonce n2 and biometric authentication request. It then waits for the biometric data to be sent to. In order to verify the live presentation of the user, the BAS sends the message that acquires the verification data. This message includes the newly generated nonce n3 and verification data request. The message is signed by the bank to specify the origin of the message. To secure the message and the validation checking purpose, the nonce, verification data and the signed package are encrypted by the public key of the TPM. The BAS expects to receive the biometric data and secret verification data sent from the user's workstation. Upon receipt, it deciphers the message, checks the validity of the data and performs the user's biometric verification. The matching result, user name and the nonce n1 which is received when the BAS has accepted the authentication result are signed by the BAS so that the recipient can validate the origin of the message. The ProVerif model of the BAS process is shown below:

```
let BAS =
 in(c,(uyName,amounty,accty,BioAuthReqx,nxx1));
 new n2;
 out(c,sign((reqBD,n1),skBAS);
 in(c,msg11);
 let (=n2,=uyName,signBD) = dec(msg11,skBAS) in
 let (BDReceived) = checksign(signBD,pkTPM) in
 new reqVD;
 new n3;
 let msg12 = sign((reqVD,n3),skBAS) in
 let msg13 = enc((reqVD,n3),pkTPM) in
 out(c,(msg12,msg13));
 in(c,(msg14,msg15));
 let (VDReceived,=BDReceived,=n3) =
 dec(msg12,skBAS) in
 let (=VDReceived,=BDReceived,=n3) =
 checksign(msg15,pkTPM) in
 let matchresult = ok in
 let msg16 = sign((uyName,amounty,accty,
              matchresult, nxx1) in
 out(c,msg16);
```

C. Workstation Process

The user's workstation initiates the communication by sending a transfer request to the bank. It then receives a request for biometric authentication and the nonce n1 from the bank. The workstation process forwards this message to the BAS. It then receives the authentication challenge and the nonce n2 from the BAS. The user places his biometric data on the sensor. This results in generation of the biometric data in ProVerif. His biometric data is signed by the TPM to guarantee its origin. The username, the nonce n2 and the signed biometric data are encrypted by the BAS's public key. This message is supplied to the BAS. The workstation process receives the request for the verification data. It then obtains this data from the user and sends it out. It

expects to receive the biometric matching result. The workstation process performs the transfer transaction by sending the relevant information to the bank in encrypted format. The transfer transaction is sent out together with the authentication result. The described user's workstation activities are illustrated in ProVerif as following

```
let WorkStation =
 in(c,uName,amount,acct)
 out(c,uName,amount,acct);
 in(c,(BDReqx,nx2));
 out(c,BDReqx);
 in(c,BDin);
 out(c,enc(nx2,uName,BDin),pkBank));
 in(c,msg3);
 let msg4 = dec(msg3,skTPM) in
 let (reqVD,nx3) = checksign(msg4,pkBank) in
 out(c,(reqVD,nx3));
 in(c,VDin);
 out(c,enc((VDin,BDin,nx3,sign((VDin,BD,nx3),
                    skTPM)),pkBank));
 in(c,matching);
 let msg10 = enc((uName,amount,acct,matching),
           pkBank)
 in(c,transfResult);
```

D. Bank Process

The Bank process represents the transfer transaction. It first receives the transfer request from the user or local's workstation. As a response, it then generates a nonce n1 and sends it with the authentication request. The bank waits for the reply message which is expected to be an authentication result. The message that the bank receives is encrypted by the public key of the TPM. It then deciphers the message; it checks the validity of the message by checking whether the first nonce is the same as the one it sent to the workstation. If so, the bank checks the signature of the message by checking whether it came from the BAS. The bank checks the matching result. If the result is positive, the bank then performs the transfer transaction. To verify the correctness of the protocol and analyse an attack to the protocol, the bank's function are modeled as

```
let Bank =
 in(c,(uxName,amountx,acctx));
 new n1;
 new BioAuthReq;
 out(c,sign((req,BioAuthReq,n1),skBank);
 in(c,msg1);
 let (=n1,=uxName,=amountx,=acctx) =
     dec(msg1,skBank) in
 let (=uxName,=amountx,=acctx,
    matchresultreceived,=n1) =
    checksign(msg2,pkBank) in
 If matchresultreceived = ok then
 out(c,acctx);
```

E. U Process

The U process represents the user's activities in the protocol. Basically, the user presents the user's biometric data for the authentication process. To secure his data, the user should be trusted with the biometric reader he is working with. He has verified the verification data which is sent from the TPM before he places his biometric data for the authentication process. The ProVerif model of the user's actions is illustrated in the U process. In this model, the U process generates the user's biometric data and sends the verification data to the channel. The verification data will be used to verify against with the value that the BAS knows. Therefore, this can be checked whether the message is sent from the legitimate user or an attacker. The U process is waiting for the request from the workstation to present his biometric data and verification data. The user verifies the verification data if he is satisfied with the data, the machine is trusted and he then presents his biometric data which in turn sends to the channel. The ProVerif model of these activities is modeled as

```
let U =
 in(c,(n,amt,acc));
 out(c,(name,amt,accout));
 in(userVD,VDq);
 out(userVD,VD).
```

F. Main Process

In order to analyze the protocol, all of the modeled processes must be run concurrently. The main process generates the keys for each process, these keys including public/private key pairs of the BAS, TPM and bank. The BAS process, the Bank process the user's workstation process and the U process are replicated and executed. The legitimate user, Bob, is exposed to the channel. An attacker Alice is used in the ProVerif model to verify whether the protocol manipulates with an attacker or not. To check the security the protocol promised, the account of the legitimate user and the account of an attacker are revealed to the protocol. ProVerif manipulates the messages in the channel to check against the requested *query attacker* to verify if any attack to the protocol is found.

```
process
 new skTPM;
 let pkTPM = pk(skTPM) in
 new skBAS;
 let pkBAS = pk(skBAS) in
 new skBank;
 let pkBank = pk(skBank) in
 out(ch,pkTPM);
 out(ch,pkBAS);
 out(ch,pkBank);

 !WorkStation | !Bank | ! BAS |
 (let name = AliceName in
 let amount = AliceAmount in
```

let account = AliceAcct in |U) |
(let name = BobName in
let amount = BobAmount in
let account = BobAcct in |U)

V. Analysis of the Model

The three desirable properties of the biometric authentication protocol are verified: the privacy of biometric data, liveness, and intentional authentication. The privacy of the biometric data is analysed to ensure that the protocol does not have risk of spreading around the user's biometric data without restriction. The ProVerif model query attacker*: BD* is used to analyse whether an attacker could intercept the data successfully.

The protocol must be guaranteed that it denies an access from the artificial biometric. The paper models Alice, an intruder, holding an artificial biometric data e.g. rubber finger of legitimate user, Bob, can obtain the positive authentication result as if she is Bob. The ProVerif model query attacker*: Alice* is analysed.

Since the protocol is used for a particular purpose, money transfer, the intentional authentication of this protocol can be illustrated as the money is transfer to the correct account for the correct amount as the user wishes. The analysis of the intentional authentication property for this protocol refers to whether an attacker can capture the authentication result and use it to transfer money by posing as the legitimate user. The ProVerif model to check that if the bank process exposes AliceAccount to the public channel, the attack is found. The model in ProVerif query attacker: AliceAccount is verified. Alice cannot intercept and manipulate the transferred message to transfer the money to her account.

The verification result illustrates that the protocol is secure for use in online money transfer in a biometric authentication situation. The protocol accomplishes all the three properties of the protocol.

VI. Summaries

This paper proposes a remote biometric authentication protocol. The protocol uses online banking to illustrate the protocol. The proposed protocol guarantees three properties: privacy of biometric data, liveness and intentional authentication. In order to secure the biometric data, the TPM is used within the user's workstation. This enhances the security level of the protocol. The user is assured that the workstation and the biometric reader he is using will not manipulate his data and request. The signatures are used to guarantee the origin of the messages. The public key encryptions are applied to secure the messages. The positive results from the verification show that the protocol holds the three security requirements. Therefore, the proposed protocol guarantees the certain level of security when it is used in unsupervised condition.

References

[1] A. Salaiwarakul and M. Ryan, "Verification of integrity and secrecy properties of a biometric authentication protocol," in *Proc. the 4th Information Security Practice and Experience Conference*, 2008, pp. 1-13.

[2] A. Salaiwarakul and M. Ryan, "Analysis of a biometric authentication protocol for signature creation application," in *Proc. the 3rd International Workshop on Security*, 2008, pp. 231-245.

[3] L. Chen, S. Pearson, and A. Vamvakas. (2002). Trusted Biometric System. [Online]. Available: http://www.hpl.hp.com/techreports/2002/HPL-2002-185.pdf

[4] Tusted Computing Group. TPM Specification version 1.2 Parts 1-3. (2009). Available: http://www.trustedcomputinggroup.org/resources/

[5] D. Dolev and A. C. Yao, "On the security of public key protocols," in *Proc. 22nd IEEE Symposium on Foundations of Computer Science*, 1981. pp. 350-357.

[6] B. Blanchet, ProVerif: Automatic Cryptographic Protocol Verifier User Manual, 2005.

[7] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," in *Proc. the 28th ACM SIGPLAN-SIGACT symposium on Priciples of programming languages*, 2001, pp. 104-115.

Anongporn Salaiwarakul is currently a lecturer at the department of computer science and information technology, Naresuan University, Phtisanuloke, Thailand. She awarded a Ph.D in computer science from university of Birmingham, 2009, M.Sc in computer science from Chulalongkorn university, Thailand, in 2002 and B.Sc. in computer science from Assumption university, Thailand in 1996. Her research interest includes computer security, semantic web and ontology.