BioPKI model and Remote Access Control using Bio-Etoken in BioPKI System

NGUYEN Thi Hoang Lan
School of Information and Communication Technology,
Hanoi University of Technology
Email: lannth-fit@mail.hut.edu.vn

NGUYEN Van Toan
School of Information and Communication Technology,
Hanoi University of Technology
Email: toannv-fit@mail.hut.edu.vn

Abstract—— **In a network, for remote accessing to a database server (DB Server) user usually has an account with a username and a password. But in fact, the password can be lost, cracked, stolen and the authentication process can be attacked (man-in-the-middle attack…). Current approach for BioPKI system based on physiological characteristics of persons, known as biometrics, provide solutions to security problems. In this paper, we present a model of BioPKI system using embedded devices and an application for remote access control. The BioPKI infrastructure could provide multi-secure layers with Bio-Etoken, Bio-cryptography protocol, Digital Signature to enhance the security of remote authentication process. The application can also against the man-in-the-middle attack on the network, the forgery and denial of user. The experimental results of BioPKI system are promising.**

***Keywords*— Biometric Security System, BioPKI System, Remote Access Control, Bio-Cryptography Protocol, Bio-Etoken**

I. INTRODUCTION

Nowadays the public key infrastructure (PKI) is common in e-transaction and developed in many applications. The PKI depends on confidentiality of private key, so the most difficult and crucial problem in PKI system is the Private Key protection. Recently a numerous researchers have studied and developed strong combinations of the two emerging technologies of biometrics and PKI. Biometrics are about measuring the personal feature based on his/her physiological or behavioral characteristics such as fingerprint, hand geometry, face, retina, iris, palm print, voice, signature, ADN, etc [2,6]. The integration of biometrics and PKI into a framework leads us to a system called BioPKI. By using the different types of biometrics, the various approaches to biometric security are proposed in BioPKI models. Although there are still many challenges to BioPKI technologies, biometrics authentication based security system has been proven to be effective in a large area of applications [6,9].

In practice, a secure remote authentication procedure has been usually based on a pair of username/ID and password provided by the system. But passwords are vulnerable, they can be cracked, guessed, key-logged, stolen or deliberately shared. Moreover, the remote authentication process also can be attacked. If the process is not secure, the credentials can be captured when they are sent over the network. Even if it's been protected by a secure connection, there are several attacking methods can be used to gain illegal access to the system. Several solutions for this problem have been proposed. One of the applications based on BioPKI system is remote access control which can be needed anywhere. In the context of BioPKI system, a true personal authentication can only be archived through their biometrics. The BioPKI solution can against the attackers as man-in-the-middle (MITM).

In this paper, we propose a model for implementing of BioPKI system and an application for remote access control based on BioPKI infrastructure. In BioPKI system, personal authentication is stronger by using Bio-Etoken combined with digital signature and Bio-Cryptography Protocol. The paper is organized as follow: section 1 introduces to problem, in section 2 we present the BioPKI system, in section 3 we present Remote Access Control solution in BioPKI system, the Bio-Cryptography Protocol and Remote Access Control process are presented in the section 4, in section 5 we present the implementation of BioPKI system and Remote Access Control in BioPKI framework with the experimental results, section 6 is about the discussion and conclusion.

II. BIOPKI SYSTEM

A. Previous works

Biometrics can be mentioned as a solution to protect Private Key instead of password in BioPKI system. Two following approaches for emerging technologies including PKI and Biometrics are proposed:

- *Private key generation from on-line biometric sampl*e

As a unique key can be dynamically generated from person's biometric sample; no storage of private key is required [5]. The advantages of this approach are obvious. It can eliminate the problem of vulnerability of private key storage. But this method provides great inconvenience to the implementation because the person's biometric samples are not unique [4,7].

- *Biometric-based key release*

In this approach, a private cryptographic key is stored as part of a user's database record, user's access privileges, that is only released upon a successful biometric authentication [4,7,8,10]. The method can eliminate the great inconveniences of the previous method, but the potential loss of biometric data can be an important security challenge in this system. The biometric key generation algorithms have been developed [7].

B. *Model for implementing BioPKI System*

Following the second approach, we proposed a BioPKI model in which the Biometric Encryption Keys (BEK) are generated and used to protect the private keys in PKI framework [11]. The BEKs have generated in two phases of BioPKI system: Biometric Enrollment for issuing certificates and Biometric Verification for using private key.

The characteristics of our BioPKI system are:

- It requires enrollment of user's biometric templates for certificate registration. In this phase, by using fingerprint scanner the live biometric template is captured. Then the Biometrics Encryption Key will be generated for issuing certificates. The BEK is used to protect accessing to private key

- It requires the live biometric template for BEK matching in the authentication process. If matching is successful, Private Key is released and can be used for the target applications.

- The user's Private Key and Biometrics Encryption Key (BEK) are securely stored in an embedded device called Bio-Etoken from which the certificate is issued

Developing a BioPKI model with embedded technology we propose a model for implementing BioPKI system that is illustrated in Fig.1.

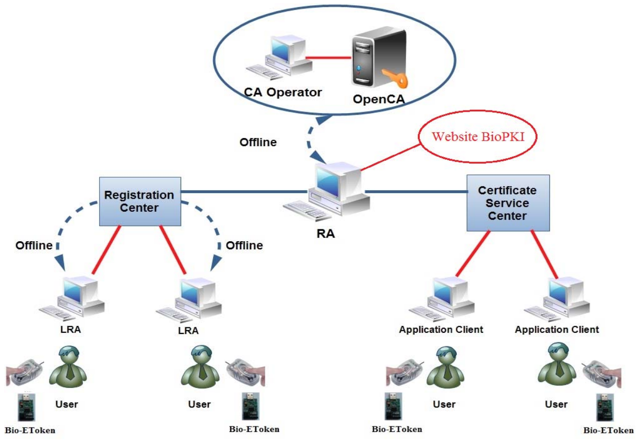

Fig.1. Model for implementing BioPKI System

- Certification Authority (CA): is responsible for certificate management and services for issuing, revoking, extending certificates in PKI core. CA includes two parties:

- **OpenCA:** This is a CA-PKI which is developed on OpenCA environment (Open Source out-of-the-box). In the BioPKI system, OpenCA provides services of PKI core and an administration interface.
- **CA-Operator:** This is a management PC tool for administrator to manage OpenCA activities. It sends user's certificate requests to OpenCA and gets certificates back, writes Bio-Etokens which will be delivered to user for further usage.

- Registration Authority (RA): is responsible for handling user's requests. It decides the approval of requests, receives Bio-Etokens from **CA-Operator** and delivers back to the lower system units (**LRA**s) and finally to system users. It also provides services related to certificate for users when they are using applications in BioPKI system. RA includes two parties:

- **Registration Center:** handles registration of certificate requests
- **Certificate Service Center or RA Application Server:** provides service about certificate: authenticating certificates, downloading certificate

- Local Registration Authority (LRA): is responsible for the interaction between clients (users) and **RA**s. It directly receives user requests and then sends to **RA,** delivers Bio-Etoken to each user.

- User: When one person wants to be a user of the system, he/she will come to one LRA, fill the information to a certificate request form and then he/she have to enroll his/her biometric templates. The Biometric Encryption Key will be generated. All the requests and BEK will be signed by LRA and then sent to RA for approval. After RA approved requests, RA will sign them again and sent to CA-Operator. From CA-Operator, administrator will issue the certificates from all the approved requests and write to Bio-Etoken devices which will be sent back to RA and finally delivered to user. User will use Bio-Etoken in every secure transaction in this system from now.

- **Biometric Authentication**: In BioPKI system, we have two implementations of the biometric authentication system:

- Live biometric authentication system using single fingerprint.
- Multibiometric authentication system at matching score level using two fingerprints and palmprint. The matching scores output by multiple matchers are integrated [2].

- Bio-Etoken: is an embedded device for each person in which several users' sensitive information will be securely stored. The storage structure in Bio-Etoken was secured.

A user's Bio-Etoken stores:

- User's Private Key
- User's Certificate (Public Key also)
- User's Biometrics Encryption Key (BEK)
- A PIN to activate token
- Other user's information

When a user want to use private key in some applications (Digital signature, message encryption…), his/her live biometrics template have to be captured, then his/her BEKs have to be verified online by using Bio-Etoken. If the verification is successful, his/her private key will be automatically retrieved from his/her Bio-Etoken for the applications.

III. REMOTE ACCESS CONTROL IN BIOPKI SYSTEM

A. *Remote Access Control Solution*

In the BioPKI's infrastructure, we propose a Remote Access Control solution to protect remote accessing to database server (DB Server) via network. This solution is illustrated in the following figure.

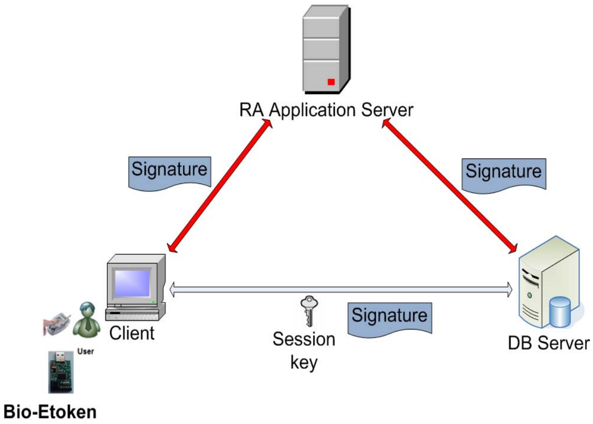

Fig.2. Remote Access Control Solution in BioPKI system

- **User**: a person has a right to remote access to DB Server. He also is a user of the BioPKI system, has a valid certificate and a Bio-Etoken device which have been issued by CA before.
- **Client:** Client machine (PC) from which user may remotely access to DB Server. This machine will be installed an application's client module which includes some functions: reading Bio-Etoken and verification, communicating with RA Application Server and DB Server, creating and verifying digital signature.
- **RA Application Server** (RAAS): Service server, one component of RA in BioPKI system. It provides services: Biometric and certificate authentication; downloading certificate; generating, managing, distributing session key to clients and DB Server.
- **DB Server**: On this server we will install application's server module which has some functions: reading Bio-Etoken and verification, communicating with RA Application Server, managing users and their activities to the database, creating and verifying digital signature.

Some pre-conditions:
Both User and DB Server are considered as end entities (users) of BioPKI system so they have to have a valid (not out of date or revoked by CA) certificate and a Bio-Etoken. BioPKI system provides certificates, tokens, and services for using issued certificates. RA Application Server will take the responsibility of session key management.

B. *Authentication using Bio-Etoken in BioPKI framework*

In our system, when a user wants to access to database server, he/she has to plug his Bio-Etoken token in the PC. After the credential (PIN) is typed in from keyboard, he has to present his biometric template online. Using his Bio-Etoken, his BEKs will be matched in local machine. If the biometric verification is success, then the private key and public key stored in Bio-Etoken will be retrieved. The system uses Private Key to sign user's credential before sending encrypted-signed credential over the network. Thus, even if password was lost, and even if token was stolen, it is very hard to forge user because hacker does not have user's live biometrics.

The data in Bio-Etoken are encrypted by AES algorithm. Then they are mixed with redundant data, and stored with another algorithm. So when data are loaded into PC, they are very secure. By using Bio-Etoken, we don't need to store users' biometric information in a central database, so we can get rid of attacking to verification process and result. The private key is also protected securely.

IV. BIO-CRYPTOGRAPHY PROTOCOL AND REMOTE ACCESS PROCESS

In our model, we also propose the combination of Bio-cryptography Protocols and using a SSL channel to against the above problems.

A. *Bio-cryptography Protocols*

In BioPKI framework the all the transactions between parties will be sent over a secure SSL channel. For one session, a Session Key (SK) is generated by RA Application Server and distributed to client and DB Server. The data exchanged between client and DB Server is signed by digital signature, and then encrypted by AES algorithm with the Session Key (SK).

When an attacker intervene between two parties, he will fail when trying to attack data exchanging on the network of BioPKI infrastructure because he does not get any participant's private key. So he cannot sign data and hope they will be verified successfully. If he captures data packets on the way, it seems impossible for him to decrypt encrypted data. If he wants to try to change them, the digital signature verification will be failed.

B. *Remote Access Control process*

The remote access control process, in BioPKI framework, is consisting of following steps:

- User uses Bio-Etoken to remote access to DB server from the client machine (PC)
- Client sends a request which includes user certificate's serial number, user ID, DB Server ID (all are registered with RAAS) and request for database login to RAAS. This request is encrypted by RAAS's public key to make sure

that only RAAS can decrypt it. Client will sign request before sending it.

- If RAAS verifies request successfully, it will respond to client. Then RAAS generates a session key with a timeout, encrypts by using client and DB Server public key, signs and sends to each side.
- Both client and DB Server will verify RAAS's signature, then decrypt by using their private key which is read from Bio-Etoken to get session key.
- Client makes another login request to DB Server which includes username, hash of login password. Client encrypts this request with AES algorithm using session key, signs and sends it to DB Server
- DB Server verifies client's signature, decrypts login request and checks database to decide if user can login or not.
- After the authentication process, the data exchange between client and DB Server will continue and all the transactions is encrypted and signed.

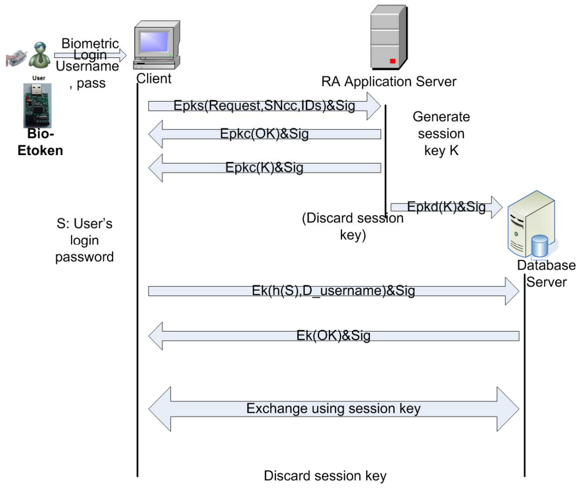

Fig.3. Sequence diagram for Remote Access Control

V. BIOPKI SYSTEM IMPLEMENTATION AND RESULTS

We performed the design and implemented the BioPKI system (prototype) in our laboratory network by using C++ language and OpenCA environment. We also deployed the certificate standard X509. The system which is built for testing the solution includes client modules PC, DB server Application modules. RAAS is a module running on RA server of the BioPKI system. RA Server runs on an IBM server XSERIES_3500, Intel Xeon 3.2GHz (4CPUs), 4GB RAM. DB Server is a MySQL server with a database for testing, runs on another IBM XSERIES server which has Intel Xeon 2.0 GHz (4CPUs), 2GB RAM with Windows Server 2003. Client PCs run on Windows XP SP2 in the same LAN with servers and have dynamic IP addresses. The testing scenario is as following.

- User 1 has his Bio-Etoken with correct username, password and his fingerprint biometric verification is successful: he successfully logs in to the network for remote access to DB Server. The speed of biometric authentication process in LAN environment is quite good (around 7s).

- User 2 has his Bio-Etoken but fingerprint biometric verification is unsuccessful, he cannot log in to the network.

- An attacker has a Bio-Etoken of any user and even if he known the user's correct username/password, but his biometric verification is not successful, he cannot log in.

VI. CONCLUSION

In this paper we present the BioPKI system and model for implementing BioPKI System (prototype) in our network laboratory. The experimental results show that by using Bio-Etoken, the private key is well-protected in different applications in BioPKI framework. We propose a solution for remote access control to DB server in BioPKI infrastructure. The experimental results are promising. Now we have to continue improve the performance of the BioPKI system and develop the applications in BioPKI framework

ACKNOWLEDGMENT

The paper is supported by the National Project KC 01.11/06-10 "Research and development of Biometric Based Network Access Control System and Information Security System BioPKI using Embedded Technology". We would like to thank to all project members and colleagues for helpful discussions and collaborations.

REFERENCES

[1] Alex Stoianow, Ann Cavoukian, Biometric Encryption: A positive – Sum Technology that Achieves Strong Authentication, Security AND Privacy, Information and Privacy Commissioner/Ontario, March 2007

[2] [Anil K. Jain and Arun Ross, "Multibiometric Systems, Journal Communications of the ACM", Vol. 47, No. 1 2004.

[3] K. Delac, M.Grgic, "A survey of biometric recognition methods", 46th International Symposium Electronics in Marine, ELMAR-2004, Zadar, Croatia. pp 1-6, June 2004.

[4] F. Hao, R. Anderson, J. Daugman, "Combining cryptography with biometrics effectively", Computer Laboratory - University of Cambridge, No. 640, 7-2005.

[5] F. Hao, C.W. Chan, "Private key generation from on-line handwritten signatures," Information Management & Computer Security - Nanyang Technological University, Singapore, 2002.

[6] Martin Drahanský, "Biometric Security System Fingerprint Recognition Technology", PhD thesis, Brno University of Technology, Czech Republic, March 2005.

[7] Uludag, Anil K. Jain et al "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Vol.92, No. 6, pp. 948-960, June 2004

[8] Yoshifumi Ueshige, "A Study on Biometrics Authentication in BioPKI", Institute of Systems & Information Technologies, KYUSHU, 2005

[9] [D.Maltoni, D.Maio, A.K.Jain, S.Prabhakar, Handbook of Fingerprint Recognition, Springer, New York, 2003.

[10] W. J. Scheirer and T. E. Boult, "Bio-cryptographic protocols with bipartite biotokens", Biometrics Symposium (BSYM)Tampa, Florida, 23-25 September 2008.

[11] [Thi Hoang Lan NGUYEN , Quang Duc TRAN , Tu Hoan NGUYEN, "A Biometrics Encryption Key Algorithm to Protect Private Key in BioPKI Based Security System", Proceeding of ICICS 2009 (IEEE 7th International Conference on Information, Communications and Signal Processing), Macau, 8-10 December 2009