Biometric Certificate on Secure Group Communication

Kun-Hee Han[1*]
[1*]Division of Information and Communication, Baekseok University

Abstract Security is a primary concern in group communication, and secure authentication is essential to establishing a secure group communication. Most conventional authentications consist of knowledge-based and token-based methods. One of the token-based methods is a X.509 certificate, which is used under a Public Key Infrastructure (PKI); it is the most well-known authentication system in a distributed network environment. However, it has a well-known weakness, which only proves the belonging of a certificate. PKI cannot assure identity of a person. The conventional knowledge-based and token-based methods do not really provide positive personal identification because they rely on surrogate representations of the person's identity. Therefore, I propose a secure X.509 certificate with biometric information to assure the identity of the person who uses the X.509 certificate in a distributed computing environment.

Key Words : Secure certificate, secure authentication, network security.

1. Introduction

Group communications have been developed explosively through the Internet since the World Wide Web was invented. Actually, computer networking was started from early in 1960s. At that time the group communications was text-based communications such as Newsgroups, Mailing lists, and text-based chatting. The Internet has provided more user friendly interfaces for people who want to communicate with each other. Due to user friendly and graphical interfaces, group communications have been developed in popularity with the development of the Internet.

A local area network is a computer network covering a small local area. The Internet is a collection of all interconnected local area networks. There are neither global administrations nor control systems on the Internet. In general, the network is not secure because an adversary may try to eavesdrop messages over the network while messages are being transferred. Transferring messages over the network are not guaranteed to be delivered to the destination nor message integrity. Therefore, security plays a major role in group communication over the insecure network. Due to insecure networks, the Public Key Infrastructure (PKI) was proposed for message integrity over the insecure networks. If a PKI is being used, then a secure group communication is guaranteed. Nevertheless, a secure authentication problem still has remained unsolved questions, in that, what factors must be identified for a secure user authentication.

The most popular authentication scheme is a certificate-based authentication which is called "something you have." A user who has a proper certificate that is issued by a Trust Third Party (TTP) is granted as a legitimate user. There is one premise that all users must agree to trust the TTP in a

Received 2014-10-29 Revised 2014-11-10 Accepted 2014-11-17

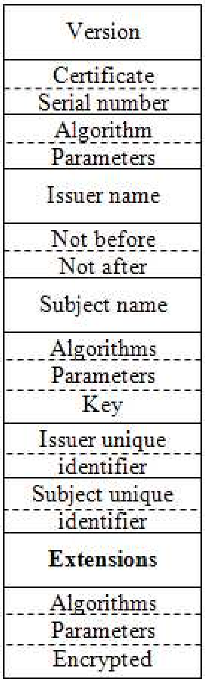
*Corresponding author: Kun-Hee Han (hankh@bu.ac.kr)

certificate-based authentication system. Even though all users agree to trust the TTP, eventually the TTP will only be able to verify the ownership or belonging of the certificate [8]. This is a major problem in a certificate-based authentication. To address this problem, we propose a secure certificate with biometric information to compensate for the weakness of a certificate-based authentication.

2. X.509 Certificate with Biometric Information

There are extensions on the X.509 v4 standard certificates. Users can define their own extensions and include them in certificates they issue. These extensions are called private, proprietary, or custom extensions and they carry information unique to their organization or business [9]. In this research, a user's biometric information as a fingerprint will be put into the extension of X.509 certificate version 4 or higher for the additional assurance of user authentication. I propose and prove secure authentication in a certificate-based authentication system by implementing a user's biometric information on the extension of a conventional certificate. A user's biometric information is an additional security feature on a X.509 version 4 certificate in order to identify a person. This research approach is based upon identifying a person. Such an approach supports user authentication by focusing on "who you are" and "what you have". Therefore, we expect that our proposed authentication enhancements have the potential to reduce the risks to participants in group communications, protect users' privacy, and ultimately improve trust between community users.

The general format of an X.509 version 4 certificates is shown in Figure 1, below. It can be seen that the certificate contains a version, a serial number, the issuer name, a signature algorithm identifier, a subject name, the public key information, the issuer's unique identifier, the subject's unique identifier, any extensions, and the CA's signature [1]. I make use of the option to include extensions to the certificate to improve security by providing more stringent rules for authentication. Specifically, we propose that digital certificates be issued with a user's biometric information as a fingerprint included in the "extensions" portion of the digital certificate.



Version

Certificate
Serial number

Algorithm
Parameters

Issuer name

Not before
Not after

Subject name

Algorithms
Parameters
Key

Issuer unique identifier

Subject unique identifier

Extensions

Algorithms
Parameters
Encrypted

Fig. 1. Format of X.509 Version 4 Certificate

The authentication process we propose is depicted in Figure 2. An example of X.509 certificate is shown in Figure 3. Suppose two network parties, Alice and Bob, agree to communicate with each other. When Alice's system initiates contact with Bob's system, his X.509 digital certificate, which includes his biometric information in the "extensions" portion of the certificate. To verification of the Bob's identity, Alice requests the certificate authority to match with the registered Bob's template and the template on the extension of the Bob's certificate. After matching, the matching score comes out and then the system can validate Bob's identity and his certificate with his biometric information.

The fact that users may desire to participate in the virtual community from a variety of locations, on a

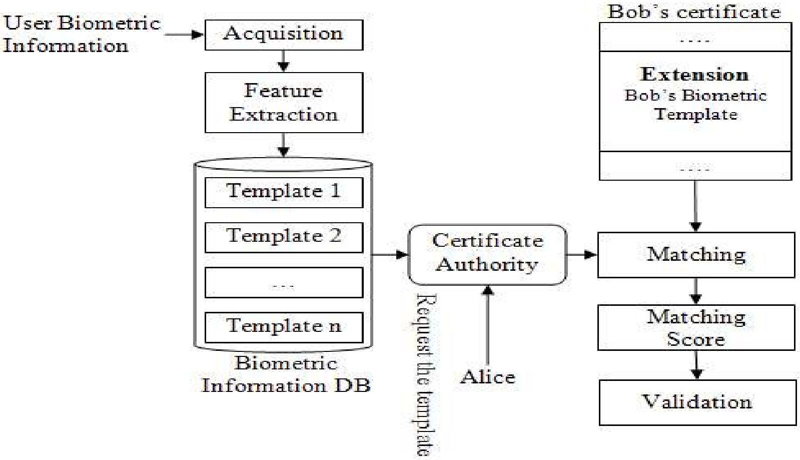


Fig. 2. Block Diagram for the Overview of X.509 Certificate with Biometric Information

variety of systems, and with a variety of different devices is not a significant issue. While biometric information is specifically identified with a actual person who is participating in a group communication.

By using the model presented here, biometric certificate-based authentication becomes a strong solution to the security problems posed by malicious users in group communications. The application of such a technique has the potential to influence users' trust perceptions and further aid the growth of group communication.

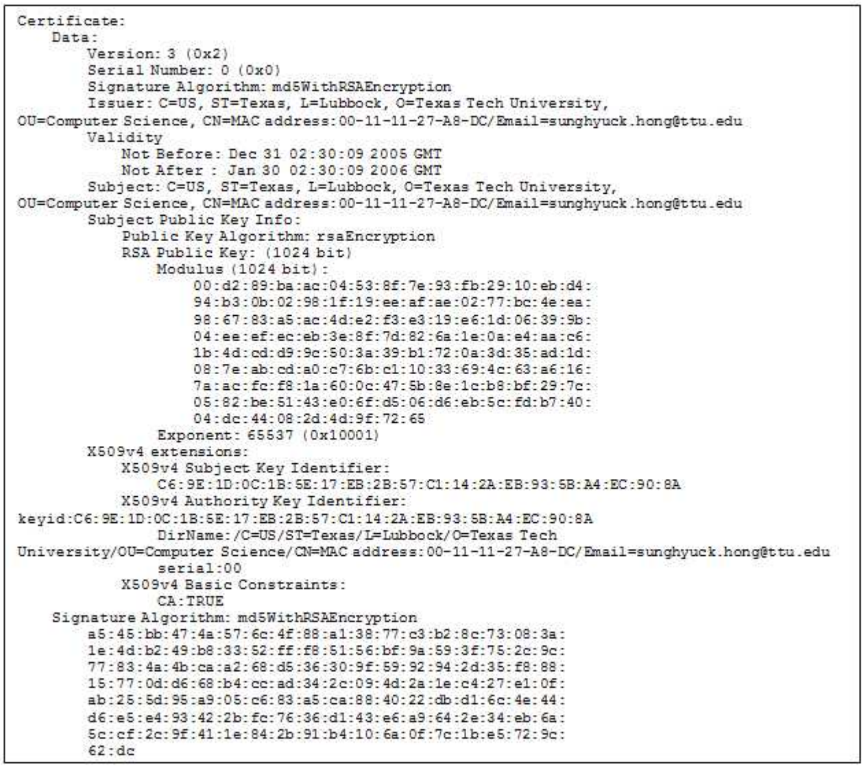
3. Performance Validation

Tradeoffs always exist between security and performance. System performance can be degraded when there is an overemphasis on security. To ensure that our proposed authentication scheme enhances security without appreciably degrading system performance, we have conducted tests comparing our proposed method to conventional certificate-based authentication by measuring the overhead introduced. The authentication processes are generally also a performance bottleneck since other security procedures which are authorization and access control cannot proceed unless the identifications of those involved can be established [6]. Therefore, it is important to measure the overheads in the proposed authentication for proving a secure and efficient authentication.

The overhead is given by the sum of execution costs and communication latencies. The overhead in conventional certificate-based authentication is determined by the encryption algorithm (i.e., RSA [2], DES [3], Blowfish [4], and RC2 [5]), variable key sizes (often ranging from 40 bits up to 2,048 bits), and computing power (determined by the type of CPU and memory size).

There is not a dramatic difference between the time required to authenticate a user using conventional authentication and the time required using a certificate with a biometric-based authentication.

This reality is demonstrated in Fig. 4 which shows that decrypting the certificate takes the longest share of time while the additional step of verifying the templates is relatively little time. The total elapsed times to complete authentication in our proposed authentication scheme are not appreciably different from the times required in conventional authentication. The proposed scheme only took 2.4 msecs more than the conventional certificate-based authentication. Based



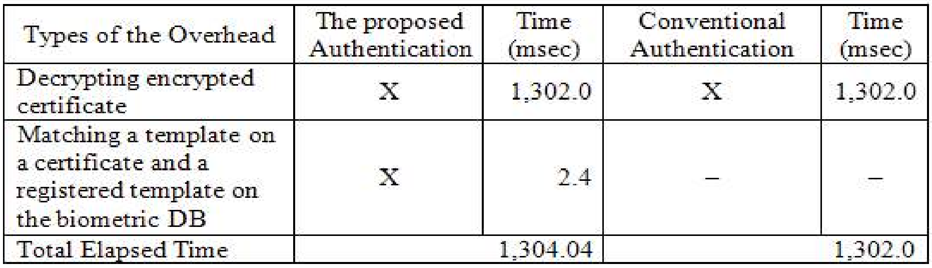
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=Texas, L=Lubbock, O=Texas Tech University,
OU=Computer Science, CN=MAC address:00-11-11-27-A8-DC/Email=sunghyuck.hong@ttu.edu
        Validity
            Not Before: Dec 31 02:30:09 2005 GMT
            Not After : Jan 30 02:30:09 2006 GMT
        Subject: C=US, ST=Texas, L=Lubbock, O=Texas Tech University,
OU=Computer Science, CN=MAC address:00-11-11-27-A8-DC/Email=sunghyuck.hong@ttu.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:d2:89:ba:ac:04:53:8f:7e:93:fb:29:10:eb:d4:
                    94:b3:0b:02:98:1f:19:ee:af:ae:02:77:bc:4e:ea:
                    98:67:83:a5:ac:4d:e2:f3:e3:19:e6:1d:06:39:9b:
                    04:ee:ef:ec:eb:3e:8f:7d:82:6a:1e:0a:e4:aa:c6:
                    1b:4d:cd:d9:9c:50:3a:39:b1:72:0a:3d:35:ad:1d:
                    08:7e:ab:cd:a0:c7:6b:c1:10:33:69:4c:63:a6:16:
                    7a:ac:fc:f8:1a:60:0c:47:5b:8e:1c:b8:bf:29:7c:
                    05:82:be:51:43:e0:6f:d5:06:d6:eb:5c:fd:b7:40:
                    04:dc:44:08:2d:4d:9f:72:65
                Exponent: 65537 (0x10001)
        X509v4 extensions:
            X509v4 Subject Key Identifier:
                C6:9E:1D:0C:1B:5E:17:EB:2B:57:C1:14:2A:EB:93:5B:A4:EC:90:8A
            X509v4 Authority Key Identifier:
keyid:C6:9E:1D:0C:1B:5E:17:EB:2B:57:C1:14:2A:EB:93:5B:A4:EC:90:8A
                DirName:/C=US/ST=Texas/L=Lubbock/O=Texas Tech
University/OU=Computer Science/CN=MAC address:00-11-11-27-A8-DC/Email=sunghyuck.hong@ttu.edu
                serial:00
            X509v4 Basic Constraints:
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
        a5:45:bb:47:4a:57:6c:4f:88:a1:38:77:c3:b2:8c:73:08:3a:
        1e:4d:b2:49:b8:33:52:ff:f8:51:56:bf:9a:59:3f:75:2c:9c:
        77:83:4a:4b:ca:a2:68:d5:36:30:9f:59:92:94:2d:35:f8:88:
        15:77:0d:d6:68:b4:cc:ad:34:2c:09:4d:2a:1e:c4:27:e1:0f:
        ab:25:5d:95:a9:05:c6:83:a5:ca:88:40:22:db:d1:6c:4e:44:
        d6:e5:e4:93:42:2b:fc:76:36:d1:43:e6:a9:64:2e:34:eb:6a:
        5c:cf:2c:9f:41:1e:84:2b:91:b4:10:6a:0f:7c:1b:e5:72:9c:
        62:dc
```

Fig. 3. Biometric Information on X509 version 4 Certificate

on these experimental results, we conclude that the increase in overhead resulting from biometric information is ignorable.

4. Conclusions

To overcome the well-known weakness in a certificate-based authentication, we proposed a certificate-based authentication with biometric information which is added into the extension area of X.509 version 4 certificate so that each network party can identify other network parties and verify reality on information in a certificate. To add a biometric template transformed into a binary form on a certificate is easy. However, it will have a ripple effect on establishing a secure user authentication.



Types of the Overhead	The proposed Authentication	Time (msec)	Conventional Authentication	Time (msec)
Decrypting encrypted certificate	X	1,302.0	X	1,302.0
Matching a template on a certificate and a registered template on the biometric DB	X	2.4	–	–
Total Elapsed Time	1,304.04		1,302.0	

Fig. 4. The Proposed Biometric-based Authentication vs. Conventional Authentication overhead

Security is in inverse proportion to system performance. No matter how secure system exists, if the overall system performance is low, then the system usability will be degraded. Therefore, the balance between the two factors must be considered. According to the experimental results, the total overhead times to complete user authentication in the proposed authentication scheme are not appreciably different from the times required in a conventional certificate-based authentication.

The contribution of this work is mainly twofold: 1) I developed and proposed user biometric information as a user's identifier which can be verified by other network parties. Biometric information on a certificate can effect user's trust and lead the development of conventional certificate-based authentication. In a virtual community, the authenticity of personal information such as name, organization, and mailing address is neither provable nor trustful. From this point of view, biometric information is important authentication factor in a virtual community and it will contribute to develop a virtual communication. 2) The proposed research provided a different paradigm for user authentication, so called “who you are” not something you have, and something you know. Therefore, the new authentication factor can be applied for a future network environment, and a system developer can select the best authentication factor. 3) The last, the development of a virtual community will lead to develop online business markets. According to [7], identity theft now ranks as America's fastest-growing crime, claiming nearly 10 million victims in just the last 12 months and at a cost of more than $53 billion. A virtual community is facing the same problem as the real world. From the business point of view, if secure authentication will be established, then the unnecessary cost lost can be prevented and will develop the activity of a virtual communication.

REFERENCES

[1] A. Menezes, P. Van Oorschot, & S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996, pp. 286-287.

[2] Rivest, R.L., Shamir, A., & Adleman, L, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 26(1), 1978, pp. 96-99.

[3] E. Biham, A. Shamir, “Differential Cryptanalysis of the Data Encryption Standard,” Springer Verlag, 1993.

[4] B. Schneier, “Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish),” Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, pp. 191-204, 1994.

[5] L. R. Knudsen, V. Rijmen, R. L. Rivest, M. J. B. Robshaw, “On the Design and Security of RC2,” Fast Software Encryption 1998, pp. 206 - 221.

[6] L. Gong, “Increasing Availability and Security of an Authentication Service,” IEEE Journal on Selected Areas in Communications, vol. 11, no. 5, June 1993.

[7] Berni Dwan, “Identity theft,” Computer Fraud & Security, vol. 2004, Issue 4, pp. 14-17, Apr. 2004,

[8] P.K. Janhandhu, M.Y. Siyal, "Novel biometric digital signatures for Internet-based applications," Information Management & Computer Security, vol. 9, no. 5, pp 205-212, 2001.

[91] Santesson, S. (2005). X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities, The Internet Society.

저 자 소 개

한 군 희(Kun-Hee Han) [종신회원]

- 2000년 2월 : 충북대학교 박사
- 2001년 3월~ 현재 : 백석대학교 정보통신학부 정보보호 전공 교수

<관심분야> : 데이터베이스, 운영체제, 정보보호, Network Security, 이동통신보안