그룹 통신을 위한 안전 MAC 주소 기반 X.509 인증서에 관한 연구

Secure MAC address-based Authentication on X.509 v3 Certificate in Group Communication

홍 성 혁*
Sunghyuck Hong

요 약

X.509 인증서 확장영역에 사용자 MAC 주소를 추가함으로써 더 신뢰성 있는 사용자 인증을 제공한다.
사용자 MAC 주소를 인증서에 첨가해도 통신 퍼포먼스에 영향을 미치지 않는 것을 시연하였으며, 간단한 MAC주소 첨가로 인해 향상된 사용자 인증을 기대한다.

Abstract

I propose adding users'Media Access Control (MAC) addresses to standard X.509 certificates to provide more secure authentication. The MAC address can be added by the issuing Certification Authority (CA) to the "extensions" section of the X.509 certificate. I demonstrate that when two users with MAC address information on their digital certificates communicate, the MAC address on the first user's certificate can be easily verified by the second user. In this way, security can be improved without markedly degrading system performance and the level of initial trust between participants in virtual communities will be improved.

☞ KEYWORD : Access Controls, Authentication, Internet Security

1. Introduction

Virtual communities on the Internet are exploding in popularity. Discussion groups, blogs, online text-based chat groups, and online video conference groups – to name only a few –are growing at a dramatic rate. Furthermore, the potential for continued growth of these communities is tremendous. As Internet usage continues to grow throughout the world, and as online communication becomes more common, virtual communities are poised to become an integral part of social and economic interaction in the Internet age.

Virtual communities are growing, in part, because they are free of the spatial and temporal constraints that often limit the growth of "real"communities of users who interact face-to-face. One consequence of asynchronous, anonymous, aspatial communication in virtual communities is that identification and authentication of users are necessary –and often challenging or problematic. It is relatively easy for malicious individuals to impersonate someone or eavesdrop on messages transmitted over a network. User authentication in virtual communities is thus a major concern [1]. The lack of security features – features that foster trust and embolden individuals to

* 정 회 원 : Texas Tech University
sunghyuck.hong@ttu.edu
[2007/10/24 투고 – 2007/11/13 심사 – 2008/02/04 심사완료]

participate in virtual communities – are presently a factor limiting the growth of virtual communities.

To increase security assurance, many security technologies have been developed [2][3][4]. Among the most commonly used strategies to authenticate users is the use of digital certificates issued by CAs. A CA verifies an applicant's credentials and identity, then issues a certificate in the form of a certified public key so that other parties have assurance that they may rely upon the possessor of the certificate. Generally, it is assumed that if a user trusts the CA and can verify the CA's digital signature on the certified public key, then the user can assume that the public key does indeed belong to the party identified in the certificate.

The current CA-based authentication has a well-known weakness, however. The weakness arises from the fact that the users cannot ensure that the name on the public key pair is really a true member's name. If a malicious user impersonates a legal member in the group, then other members attempt to verify whether the user's certificate belongs to the legal member by checking both the CA's public key and the public key that is encrypted by the CA's private key. There is no way to definitively prove, however, that the information on the certificate is true or false since users enter their own information; this is the main problem in certificate-based authentication.

To address this problem, we propose MAC address-based authentication [5] to compensate for the weakness of a certificate-based authentication. According to [5], user authentication is only based on the MAC address which is a physical address associated with the IP address.There is no any other authentication method. Furthermore, computing machine can be identified by the MAC address. However, a user can't not be identified by the MAC. Therefore, a MAC address itself isn't enough to identify a user. Therefore, user authentication must be combined with conventional authentication method.

Authentication methods are various. Authentication based upon physical characteristics of a user's system has been proposed by other researchers [1] but not widely implemented because of security reason. In addition, human's biometric information itself still needs to be added additional security features due to biometric accuracy. Biometric information must be transformed into a template and determined by assessment system. There is no 100% accuracy between a registered template and scanned template that users just scan his/her biometric information [6]. That is the reason that the biometric information is not widely pervaded for authentication. Such an approach supports member authentication by focusing on where a user is in addition to who a user is. Before describing the authentication scheme we have developed that can be used to improve authentication provided in standard X.509 certificates, we will briefly touch on advances in cryptography and present a model for MAC address-based authentication. We believe our proposed authentication enhancements have the potential to reduce the risks to participants in virtual communities, protect members' privacy, and ultimately improve trust between community members.

The paper is organized as follows. In Section 1, the authentication problem is introduced. Section 2 describes that authentication problem in group communication is introduced and MAC address-based authentication is explained and proposed in Section 3. In Section 4, the method of MAC address-based authentication is explained. In Sections 5, the proof of efficiency in MAC address-based authentication is explained. Finally, conclusions and future works are presented in Section 6.

2. Issues in Public Key Infrastructure (PKI)

A PKI is a system used to provide a trust relationship between network parties by issuing a certificate and enabling members to be authenticated over an insecure network. The PKI consists of the components thatare necessary to establish a trust relationship and deliver a message securely over an insecure network. The components are CA, certificate, member, Registration Authority (RA), repository, Certificate Revocation Lists (CRL), and a method of evaluating a chain of certificates from public keys that are known and trusted by the target name in advance. However, most public key based systems do not have all components [7]. Furthermore, Current group communication protocols use a self-signed certificate which has a well-known weakness arising from the fact that members cannot ensure that the name on the public key is really a true member's name [8]. Since members enter their own information there is no way to definitely prove that the information on the certificate is true or false. For secure group communication, secure member authentication and the integrity of messages must be provided among group members. To maintain secure member authentication, current self-signed certificate must have additional security features.

3. Model for Improved Authentication

The weaknesses of public key encryption can be mitigated by utilizing MAC addresses during authentication. A MAC address is 6 bytes (48-bit), expressed as 12 hexadecimal digits, with a theoretical number of addresses equal to 16^{12} (281,474,976,710,656). The first three bytes of the MAC address are a network card manufacture ID that is globally assigned by the Institute of Electrical and Electronics Engineers (IEEE) [9]. Theremaining three bytes are station ID's assigned by each manufacturer. MAC addresses are unique in any Local Area Network (LAN) at any given time. A user may change the MAC address in a network card but the new MAC address will be registered to the routing table in the router to communicate with outside networks. If a duplicated address is found, network packets will not be able to be transmitted to the duplicated address. Because of this reality, a MAC address-based identification scheme will assist in user authentication.

MAC spoofing poses a threat to effective implementation of MAC address-based authentication. ARP is not an IP-onlyor Ethernet-only protocol; it can be used to resolve many different network-layer protocol addresses to hardware addresses, although, due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses. In addition, it is used for IP over other LAN technologies such as Token Ring, FDDI (Fiber Distributed Data Interface) which provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles) [10], or IEEE 802.11, and for IP over Asynchronous Transfer Mode (ATM). IP over Ethernet networks are the most popular LANs nowadays. They use ARP, the Address Resolution Protocol, to resolve IP addresses into hardware, or MAC addresses [11].

ARP is an essential function used by a network interface card (NIC) to find the physical address of a destination NIC [12][13]. In traditional ARP, a user who needs to send data to another user will have the Internet Protocol (IP) address of the destination, but the sending NIC must use ARP to

discover the corresponding physical address. The address is obtained by broadcasting an ARP request packet that announces the IP address of the destination NIC. All stations hear the request, and the station having the corresponding IP address will return an ARP response packet containing the MAC address and IP address. The sending user's station will then include this MAC address as the destination address in the packet being sent. The sending station also stores the IP address - MAC address mapping in a table for a period of time (or until the station receives another ARP response from the station having that IP address).

During the ARP request-response sequence, MAC spoofing could happen. For example, an adversary can fool a station by sending the MAC address from a malicious network device. A false ARP response, which includes the IP address of a legitimate network device and the MAC address of the rogue device, could cause all legitimate stations on the network to automatically update their ARP tables with the false mapping. MAC addresses and IP addresses are not private; a malicious adversary can access the ARP table make them available. In light of this reality, MAC spoofing is a cause for concern in any scheme that advocates using MAC addresses for authentication. To minimize the risk posed by this tactic, Secure Address Resolution Protocol (SARP) [14] should be employed.

SARP is an enhancement to ARP that provides a special secure tunnel between each client and router that ignores any ARP responses not associated with the client on the other end of the secure tunnel. Therefore, if SARP is installed on the client side of the stations, only legitimate ARP responses provide the basis for updating ARP tables. With this enhancement, MAC address-based authentication becomes a viable avenue for improving security in virtual communities.

In sum, the use of a MAC address significantly increases the level of security in the group communication protocols and preventsa possible impersonation only if attempts at MAC spoofing are thwarted. A malicious adversary who wants to impersonate a legitimate member of a virtual community must expose his or her own physical MAC address to initiate communication. Since the exposed MAC address provides a mechanism to trace the adversary's location and thus allows the virtual community to filter out this unknown MAC address, an adversary might hesitate to impersonate a member and join the group communication. Clearly, MAC address-based authentication aids in the implementation of secure group communication and enhances strategies currently in use.

There is a prerequisite to accomplish a secure MAC address-based authentication, in which each member must use his/her own machine to communicate with others. If a user use more than one machine, he/she must register his/her MAC addresses to a group control server for authentication. More secure features always lead to more constraints. To establish secure group communication, the prerequisite must be satisfied.

4. Mac-Address based Authentication

The general format of an X.509 version 3 certificates is shown in Fig. 2, below [15]. 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 [16]. Wemake 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 MAC address included in the "extensions" portion of the digital certificate. The authentication process we propose is depicted in Fig. 3. Suppose two users, Daniel and Olivia, agree to communicate with each other. When Daniel's system initiates contact with Olivia's system, his X.509 digital certificate, which includes his MAC address in the "extensions"portion of the certificate, is transmitted to Olivia. An example of an X.509 certificate with the added MAC address information is shown in Fig. 4.

In this scenario, the MAC address in Daniel's certificate is used as a security deposit – Daniel must initially offer something of value to initiate interaction. Olivia's system validates Daniel's certificate by using the GetAdaptersInfo() function to contact Daniel's NIC card and verify that the MAC address on his certificate matches the one on his NIC card.

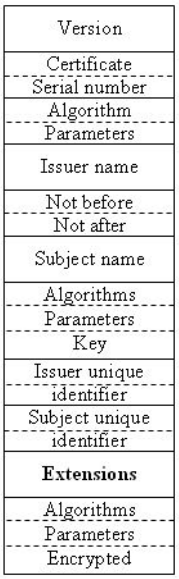

Fig. 2. Format of X.509 Version 3 Certificate

Once this process is transacted, communication between the two users can begin.

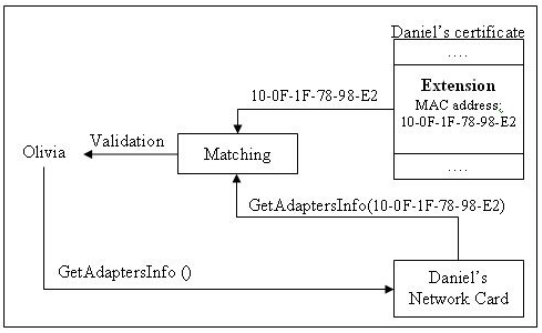

Fig. 3. Verification of MAC Address Using GetAdaptersInfo() Function

As depicted in Fig. 3 and described above, our proposed method for verifying a user's MAC address relies upon the GetAdaptersInfo()function from the C programming language, and can be implemented by any system with a C compiler. This function can be used so that each party on a network can verify the other's MAC address. The code for verifying a MAC address using this function is presented in Fig. 5, below. We believe that the inclusion of MAC address information in digital certificates, when paired with verification using the GetAdaptersInfo() function, offers significant additional assurance in verification of user identities. Thus, CAs can begin to add MAC address information to the digital certificates they issue to mitigate the risks currently endemic to interactions in virtual communities. An overview of secure group communication is shown in Fig. 6. In this Fig., users A and B request a certificate which is a public key to a CA. The CA then issuesthe public key that each user requests. Thus, each user can possessa certified public key containing the user's name, the date of issue, the MAC address, and the CA's signature.

```
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:9f: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)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                C6:9E:1D:0C:1B:5E:17:EB:ZB:57:C1:14:2A:EB:93:5B:A4:EC:90:8A
            X509v3 Authority Key Identifier:
keyid:C6:9E:1D:0C:1B:5E:17:EB:ZB: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
            X509v3 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:f9:88:
        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. 4. MAC address on X509 version 3 Certificate

```
static void GetMACaddress(void)
{
      IP_ADAPTER_INFO AdapterInformation;
      DWORD dwBufLen = sizeof(AdapterInformation);
      DWORD dwStatus = GetAdaptersInfo(AdapterInformation, &dwBufLen);
      assert(dwStatus == ERROR_SUCCESS);
      PIP_ADAPTER_INFO p AdapterInformation = AdapterInformation;
      do
      {
          PrintMACaddress(p AdapterInformation ->Address);
          p AdapterInformation = pA AdapterInformation ->Next;
       }while(p AdapterInformation);
}
```

Fig. 5. To Retrieve MAC address C Language Code

In addition, by using the aforementioned GetAdaptersInfo() function, each user in Fig. 6 can verify the other's identity and trace the other's physical location in the network using the MAC address on the certificate. If both parties possess a valid key pair (a certified public key and a private key), then they can communicate securely using the keys.

The fact that users may desire to participate inthe virtual community from a variety of locations, on a variety of systems, and with a variety of different devices is not a significant issue. While a MAC address is specifically identified with a user's NIC card, users who desire to participate in a virtual community from a variety of locations may simply register the new machine's MAC address to be authenticated by the authentication server. Thus, users are not limited to accessing the virtual community from only one machine.

By using the model presented here, MAC address-based authentication becomes a strong solution to the security problems posed by malicious users in virtual communities.

Using a MAC address leads another constraint which a user must use his/her own machine. If he/she wants to use another, he/she must register another MAC address to others. Therefore, there is a prerequisite to accomplish a secure MAC address identification, in which each member must use their own machine to communicate with others. More secure features always leadto more constraints. To establish secure group communication, the prerequisite must be satisfied. The application of such a technique has the potential to influence users' trust perceptions and further aid the growth of virtual communities.

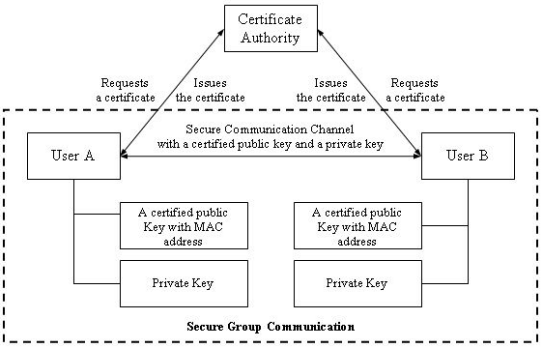

Fig. 6. Overview of Proposed Secure Group Communication

5. Improving Security without Degrading System Performance

The overhead is given by the sum of execution

costs and communication latencies. The overheadin conventional certificate-based authentication is determined by the encryption algorithm (i.e., RSA [17], DES [18], Blowfish [19], and RC2 [20]), 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).

The overhead to trace MAC addresses using the *GetAdaptersInfo()* function in our proposed authentication scheme is directly related to network latencies, including how many hops to travel between network parties, network bandwidth, the size of data packet, types of communicational protocol, and types of routing algorithms. With the exception of the number of hops, the network latencies do not affect the experimental resultsbecause they are invariable. The number of hops is a major overhead for the proposed method. More hops necessitate more transfer time to check the integrity of the retrieved MAC address.

To estimate the MAC tracing overhead, we measured the elapsed times to trace a MAC address on a SUN Ultra Sparc (SunOS Release 5.9, 270 MHz, Memory 256MB, 4GB IDE hard drive) with a 1024 bit RSA key to encrypt and decrypt the certificate. Fig. 7 shows the elapsed times to trace a MAC address for various numbers of hops.

There is not a dramatic difference between the time required to authenticate a user using conventional authentication and the time required using MAC address-based authentication. This reality is demonstrated in Fig. 7 which shows that decrypting the certificate takes the longest share of time while the additional step of verifying the MAC address adds 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.

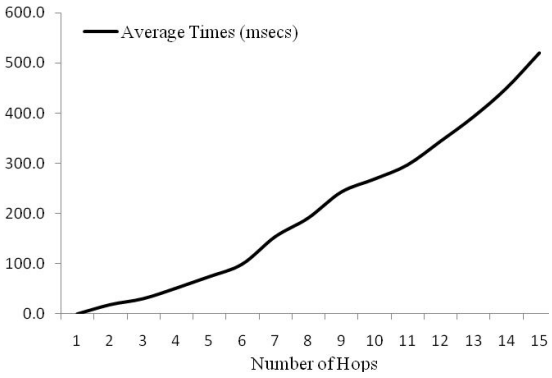

Fig. 7. Elapsed Times for Tracing a MAC address by Number of Hops.

Table 1. Proposed MAC-Based Authentication versus Conventional 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
Retrieving a MAC address from a certificate	X	2.4	-	-
Tracing a MAC address	X	209.3	-	-
Total Elapsed Time		1513.7		1,302.0

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. According to Table 1, the proposed scheme only took 209.3 msecs more than the conventional certificate-based authentication. Therefore, based on these experimental results, we conclude that the increase in overhead resulting from MAC tracing is only slight.

6. Conclusion

When participants in virtual communities agree to place their confidence in a trusted third party such as a CA, then trusting relationships between users can develop. As we have shown, security in online virtual communities can be improved by the introduction of new authentication strategies that verify a participant's physical location. Physical address-based authentication provides more assurance for trust relationships in virtual communities. A malicious individual might hesitate to join a virtual community if his or her originating physical address were able to be traced by using his or her MAC address. While there is a slight increase in the amount of overhead introduced by the integration of the MAC address into the authentication scheme, without such security enhancements, participants in virtual communities will continue to be exposed to unnecessary risk. To increase security level in group communication, MAC address-based authentication must be used with conventional authentication scheme in order to reduce risks, and we will continue to research about the security assessment in MAC address-based authentication in our future work.

Without employing strong security features, virtual communities will not fully accomplish their goal of enabling communication between members who share common interests. Virtual communities should thus have strong security features to protect members' privacy and message integrity.The attractiveness of virtual communities has been demonstrated by the vast numbers of users who have already begun to participate in them. If the security risks that are common to these communities can be reduced, opportunities for further growth can be more easily realized.

References

[1] Kohno, T., A. Broido, et al. (2005). "Remote Physical Device Fingerprinting." IEEE Transactions On Dependable And Secure Computing 2(2).

[2] N. Ferguson; B. Schneier (2003). Practical Cryptography. Wiley.

[3] J. Katz; Y. Lindell (2007). Introduction to Modern Cryptography. CRC Press.

[4] A. J. Menezes; P. C. van Oorschot; S. A. Vanstone (1997). Handbook of Applied Cryptography.

[5] S. Hong, N. Lopez-Benitez, "Media Access Control (MAC) Address-Based Group Key Authentication Scheme,"the 9th World Multiconference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA, in July 10-13, 2005.

[6] R. Smith, "Authentication from Passwords to Public Keys", Addition Wesley, 2001, pp. 211-215.

[7] Kaufman, C. P., R. and M. Speciner (2002). Network Security, Printice Hall.

[8] Hong, Sunghyuck, "Secure and Efficient Group Key Agreement Protocols," Ph.D. dissertation, August 2007.

[9] B. Mitchell, "An Introduction to MAC Address ing." Available: http://compnetworking.about.com /od/networkprotocolsip/l/aa062202a.htm

[10] Federal Standard 1037C, "Fiber distributed data interface," 2007. Available: http://en.wikipedia.org/wiki/FDDI.

[11] D. C. Plummer. An ethernet address resolution protocol. RFC 826, 1982.

[12] J. Geier, "Beware of ARP Attacks," 2003. Available: http://www.wifiplanet.com/tutorials/article.php/3112991.

[13] Eric Cole, Ronald Krutz, and James Conley, Network Security Bible, Wiley Publishing, Inc. 2005, p. 427.

[14] M. Gouda, C. Huang, "A secure address resolution protocol." Computer Networks, vol. 41, no. 1, 2003, pp. 57-71.

[15] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure: Certificate Management Protocols", RFC 2510, March 1999

[16] W. Stallings, Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall, 2002, pp. 341-342.

[17] 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.

[18] E. Biham, A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer Verlag, 1993.

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

[20] 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

◐ 저 자 소 개 ◑

Sunghyuck Hong

received his B.A. degree from Myongji University in 1995. After graduation, he worked at Hyosung Inc. in Seoul, Korea from 1995 to 1999 as a computer programmer and ERP consultant. He has a Ph.D. degree from Texas Tech University in August, 2007 major in Computer Science. Currently, he works at International Affairs in Texas Tech University as a senior program/analyst. His current research interests include secure authentication, secure group communication, biometric authentication, and key management protocol.