SMS based Advanced Sender Authentication Mechanism for Anti-Spam based on DomainKey

Jong-Won Seo[†], *Je-Gyeong Jo*[†] *and Hyung-Woo Lee*[†]

[†]Division of Computer, Information and Software, Hanshin University, Korea

Summary

Electronic mail is playing an important role for communication among Internet users. However, the value of electronic mail is being impaired by spam mails including unwanted commercial information, virus mails including malignant codes and many different forms of unnecessary information. Thus, it is urgent to develop a method of blocking spam mails fundamentally. The present study proposes a method in which an electronic mail sender receives confidential information through SMS (Short Message Service) and creates a private key/public key pair used in the DomainKey method and, in connection with the existing PGP method, the email sender is authenticated and the message is encrypted/decrypted. Because the proposed method authenticates the sender in the process of mail transmission, it can prevent spam mails.

Key words:
E-mail Authentication, PGP, DomainKey, Anti-SPAM, SMS

1. Introduction

The number of spam mails is increasing by over 200% every year, and their forms are getting more intelligent. The explosion of spam mails is increasing social and economic costs considerably in our society. According to a recent survey, the amount of social and economic costs caused by spam mails in Korea reaches 2,645.1 billion won. The number of spam mails transmitted each day is 915.04 million, and each person spends 44 hours a year to delete spam mails. In addition, spam mails increase traffic on business networks and lower the speed and the performance of networks and mail servers, and to solve these problems, costly servers have to be added unnecessarily every year.

Most of currently available spam prevention technologies use filtering based on specific words or phrases after spam mails have already been sent. Thus, filtering-based spam mail prevention on the mail receiver side cannot be a fundamental spam prevention technology, and now we need to develop an advanced spam prevention technology.

To solve the vulnerable points of existing spam mail prevention techniques, we need to authenticate senders by having senders insert their signature to their mails and to give secrecy/confidentiality to mail messages through encryption.

Thus, in order to prevent spam mails in the sending process, the present study purposed to provide functions of confirming/verifying mail senders and authenticating the senders from the receiver side while guaranteeing message integrity.

Using the technology developed in this study, spam mails are examined when they are sent, and this is expected to reduce the transmission of spam messages and prevent malignant viruses delivered through spam mails.

In this paper, Chapter 1 Introduction explains the current state of spam mails, and Chapter 2 Related Works review existing spam prevention technologies and points out problems in them. Chapter 3 Proposed Model explains the proposed model, its necessities and its spam prevention effect. Chapter 4 explains the characteristics of the proposed system through comparative analysis with existing systems. Chapter 5 Conclusions summarizes the results of this study and suggests future research topics.

2. Related Works

2.1 Existing Anti-SPAM Methods

(1) SPF(Sender Policy Framework)

A spam mail means an email unwanted in the Internet community (UBE-Unsolicited Bulk E-mail), unwanted commercial email (UCE- Unsolicited Commercial E-mail), an indiscriminate bomb mail, etc. Recently, spam mails are used as a means of commercial marketing because they are highly cost-effective as usual in the Internet marketing compared to offline advertisements. However, they are inflicting heavy losses on consumers.

This work was supported by Korea Research Foundation Grant (KRF-2005-202-D00487)
Manuscript received Feb., 2, 2007.
Manuscript revised March 28, 2007

Today's SMTP-based mail transmission structure is as in the figure below. The sender makes a message through the mail client and sends it through MTA. In the same way, the receiver receives the message from MTA based on SMTP protocol.

In this process, spam mails may take place for reasons as follows.

Receive a large number of commercial mails

- Unable to verify SMTP senders
- Senders send mails arbitrarily
- Unable to authenticate mail senders

Thus, until now, spam mails have been prevented through filtering in the process that a large number of commercial mails are sent to random receivers. However, this method cannot be a fundamental protection. The fundamental reason for the occurrence of spam mails is that mails can be sent easily by any sender. Thus, spam mails can be prevented actively through authenticating senders in SMTP and tightening security in protocol. Concerning this, existing spam mail prevention methods are as follows.

Therefore, SPF technology prevents illegal spam mails by determining whether a mail has been sent by the corresponding mail server based on the mail header.

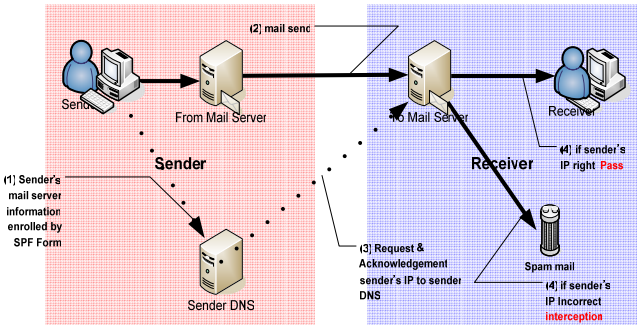

Figure 1 SPF Process

For example, if the From header of the mail is foo@spammer.com, the IP of spammer.com set in the mail through the DNS server managing spammer.com is compared with the IP in the header of the received mail, and if they are different, the mail is rejected. That is, if a mail, which is not sent by hanmail.net, is sent with its mail address changed to @hanmail.net, SPF filters the mail.

(2) Challenge-Response Filtering

C/R filtering system is a spam filtering method that responds to email messages containing the email challenge of the sender. The responded user can get normal mail service from the response. However, because the response is made to the administrator of the mail server, the authentication of the sender can be forwarded to a different person by the administrator's mistake. In addition, because of the exposure of From header, the sender's information can be spoofed.

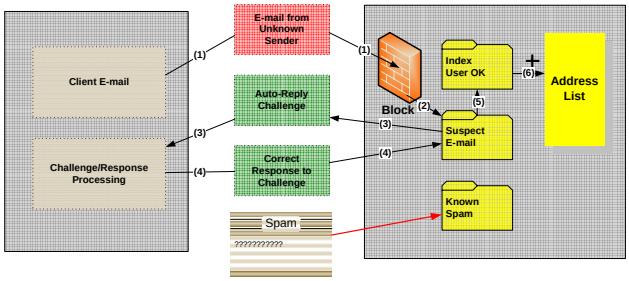

Figure 2 Structure of C/R Filtering System

2.1.3 Weak Points of Existing Spam Prevention System

Existing spam prevention systems have problems as follows. The information of the sending mail server has to be registered in SPF in advance, and the biggest problem is secondary damage that normal mails from unregistered and unauthenticated sending mail servers are blocked. In addition, small and medium businesses, which regard email marketing as their major means of advertisement, lose the important marketing channel.

Existing spam prevention technologies based on filtering respond passively/restrictively to spam mails that are getting more intelligent and complicated.

Basically, with existing SMTP protocol header information, spammers can change the information and retransmit a large number of emails easily. If sender address and titles are spoofed from mail header information, existing SMTP protocol cannot detect the trespasses. It is because existing SMTP protocol does not have any mechanism for security and safe transmission/authentication to prevent illegal spam mails from being sent. Thus, we need to study advanced techniques for improving the vulnerable points in existing SMTP protocol.

3. Analysis of Existing DomainKey Mechanism

3.1 DomainKey Sending Server Operations

Domain key-based mail authentication is made through two steps.

- Preparation step: The domain owner creates public/private keys for all messages transmitted. The public key is activated in

DNS and the private key is created and managed in the mail sending server that uses a domain key.

- Authentication step: In sending a mail, the mail system creates a digital signature for the message using the saved private key. The signature is saved in the message header and the message is sent to the mail server of the receiver.

3.2 DomainKey Receiving Server Operations

An authenticated mail is verified through three steps.

- Preparation step: The mail receiving system that uses a domain key extracts digital signature and the domain of 'From' from the message header and downloads the public key of the 'From' domain from DNS.
- Verification step: The public key from DNS is used to verify if the digital signature in the message header was created from the private key matching with the public key. This proves whether the mail was sent after the 'From' domain was approved and whether the mail header and its contents have been protected during transmission.
- Delivery step: The mail receiving system disposes the mail depending on the result of digital signature test. if the domain is verified and the mail passes other spam tests, the mail is delivered to the user's inbox. If the signature is not approved or not tested, the mail is not delivered or it is forwarded to the spam mail box.

3.3 Problems in DomainKey based Sender Authentication

In the DomainKey method, the corresponding MTA should be installed and key setting and allocation for MTA should be supported.

In DomainKey, signature for a message is created using a private key but because the signature is not for the whole content, it is possible to retransmit the created message. Accordingly, to prevent retransmission, the problem in the DomainKey method, a different private/public key pair should be applied to each message. In addition, because in the DomainKey method the contents of a mail is changed in the message transmission process, the added digital signature may not be usable any more in authentication. Thus, a re-sign process is executed or an existing method like SPF is used together.

However, as discussed above, SPF, which determines the legitimacy of the mail sender using the sender's IP address, also has a problem caused by IP spoofing. Thus, centering on MTA, this study developed a new sender authentication method through the SMS system in order to enhance the safety and efficiency of public/private key generation and management in the existing DomainKey method and to cope more effectively with retransmission and problems in the transmission process.

4. Proposed Methods

4.1 Proposed Model

Existing spam prevention systems are composed of sender IP and filtering techniques. As explained in Chapter II, however, these methods have many problems. The biggest problem is the absence of sender authentication process.

Sender verification using SMS is focused on spam mail prevention through sender authentication. Today when each individual has his or her own mobile phone, the text message service of mobile phones is used in many authentication processes. For example, micro-payments are sometimes made through mobile phone bills and the use of mobile phone authentication is increasing remarkably for credit card payments in e-commerce. This is to authenticate individuals using popularized mobile phones.

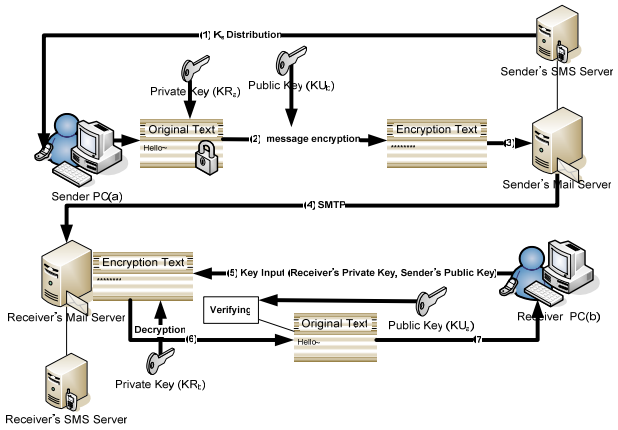

Figure 3 The architecture of the proposed system using SMS

Figure 3 shows the overall architecture of the proposed system. To send an email, the sender connects to POP3, IMAP4 and WebMail [4]. The subsequent procedure is as follows.

– Step 1: When the sender connects to Application to send a mail, it receives Ks for message encryption from the sender's SMS Server via the text message service of the sender's mobile phone. This process

uses the mobile phone information reported when subscribing for the mail service.

- Step 2: The sender signs its mail using the private key. Here, the message of the mail is encrypted together using Ks provided by SMS.
- Step 3: The sender's mail is transmitted to the sender's mail server.
- Step 4: The mail is sent by SMTP to the receiver's mail server.
- Step 5: With the encrypted message, Ks can be obtained using the receiver's private key. Therefore, the encrypted message is decrypted.
- Step 6: The receiver authenticates the sender using the sender's public key.
- Step 7: If Step 6 is carried out normally, the receiver receives the original text.

4.2 Key Generation and Allocation Process

In this study, we used SMS server for key allocation efficient in spam mail prevention using the algorithm of PGP (Pretty Good Privacy) [2]. In addition, we implemented a safer spam mail prevention system by combining sender authentication with message encryption. In the proposed method, the key allocation scenario is as follows, assuming that the private key is KRx(x=a, b), the public key KUx(x=a, b), and EP and DP are the message encryption and decryption processes, respectively, using the public key encryption method (RSA)[3].

In the proposed method, the key allocation scenario is as follows, assuming that the private key is KRx(x=a, b), the public key KUx(x=a, b), and EP and DP are the message encryption and decryption processes, respectively, using the public key encryption method (RSA)[3].

We assume that Ks is a session key used in conventional encryption, and EC and DC are encryption and decryption, respectively, using the conventional encryption method. In addition, it is assumed that the sender's and the receiver's SMS servers have the public keys of all ISP companies and individual mail server users.

The sender's SMS server generates Ks based on information from the mail server and the user, and send information on the sender's mobile phone as a SMS message. The detailed procedure is as follows.

- Step 1: User A generates basic information
  - ID_a : Composed of the sender's information (mail address, name, mobile phone number, etc.)
  - ID_b : Information on the receiver
  - N1 : A random number generated by the sender
  - Ts : Information on the period of service time
- Step 2: User A make a request to the mail server
  - Create $EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts))$
  - Join the values created above with ID_a, ID_b and Ts, encrypt them with the public key of the mail server, and send

$$EP_{KUs1}(EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts)) \| ID_a \| ID_b \| Ts)$$

- Step 3: The mail server requests key generation to the SMS server
  - The mail server decrypts the values from the user and records ID_a, ID_b and Ts.
  - Because Ts is meaningful only during the period of key use, it should be used during the corresponding time period.
  - The mail server generates random number N2.
  - With the generated number and ID_a and ID_b received from the SMS server, it requests key generation to SMS server as follows.

$$EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts)) \| EP_{KUsms}(ID_a \| ID_b \| N2)$$

- Step 4: The SMS server generates session key K_s
  - The SMS server encrypts the value received from the mail server and verifies the user's signature, and through the process, decrypt the value and generate the key.

$$DP_{KRsms}(EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts))) = N1 \| Ts \| EP_{KRa}(N1 \| Ts)$$

$$DP_{KUa}(EP_{KRa}(N1 \| Ts) = N1 \| Ts\ ,$$
$$DP_{KRsms}(EP_{KUsms}(ID_a \| ID_b \| N2)) = ID_a \| ID_b \| N2$$

  - The SMS server generates random number N3 and creates session key K_s

$$K_s = H(N1 \| N2 \| N3)$$

- Step 5: The SMS server sends information on session key K_s and other data to the mail server and the user
  - The SMS server generates a message using N2 from the mail server and sends it through the following confirmation reply procedure.

$$EP_{KUs1}(EP_{KUa}(N1 \| N2 \| EP_{KRsms}(K_s)) \| N2)$$

  - Using N1 and N2, the SMS server sends the confirmation reply to the mail server and, in this process, information on K_s is encrypted with user A's public key into the form of $EP_{KUa}(N1 \| N2 \| EP_{KRsms}(K_s))$ so that only the user can decrypt, and the mail server confirms the reply through N2.
  - In addition, for random number N3, the SMS server sends a mobile phone SMS message to the user's mobile phone.

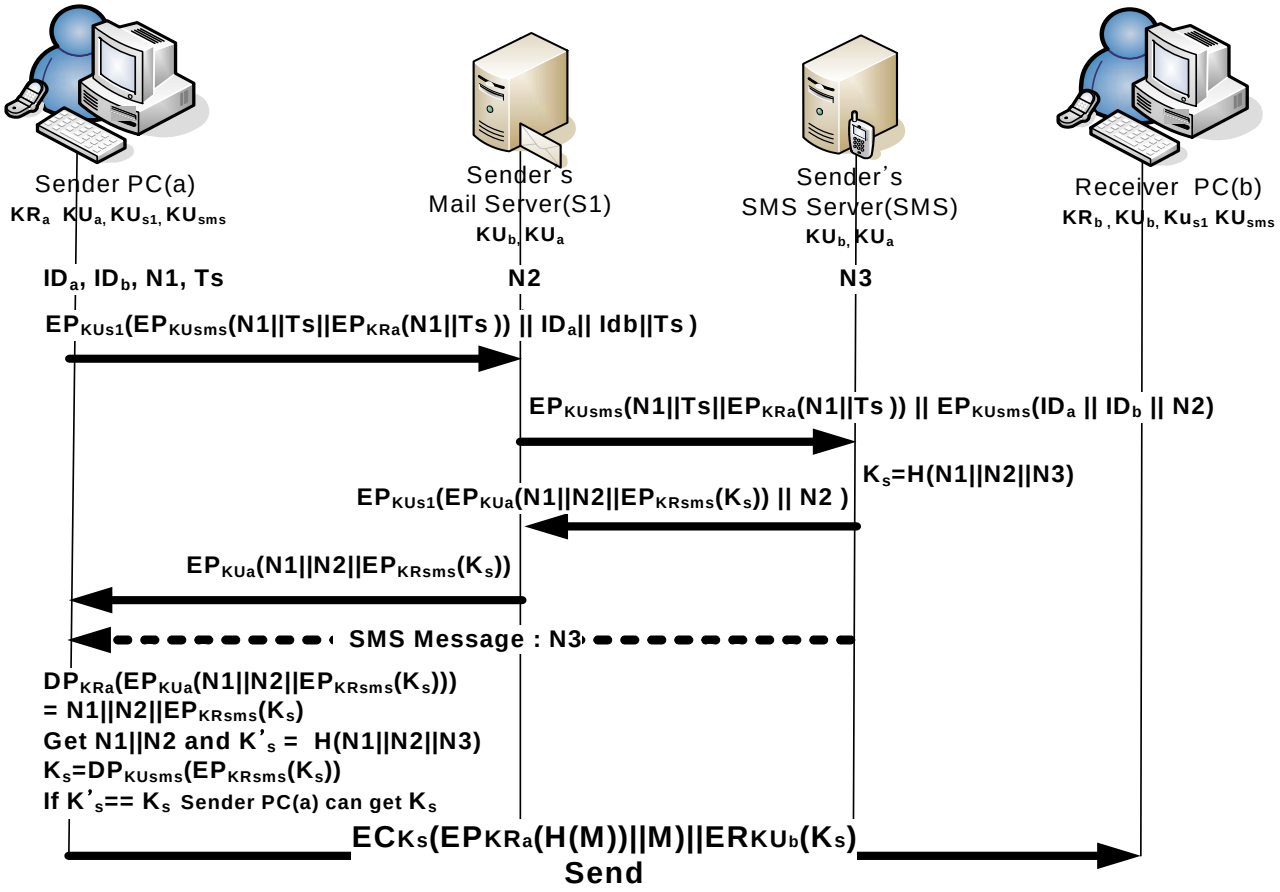

Figure 4. Proposed Authentication Mechanism

− Step 6: The mail server delivers the message from the SMS server to the user.

- Again the mail server delivers the decrypted contents of the message from the SMS server to the user. $EP_{KUa}(N1 \| N2 \| EP_{KRsms}(K_s))$

− Step 7: The user verifies the key for the message from the mail server and the SMS server and carries out the mail transmission process.

- The user verifies K_s through verification process as follows.

$$DP_{KRa}(EP_{KUa}(N1 \| N2 \| EP_{KRsms}(K_s))) = N1 \| N2 \| EP_{KRsms}(K_s)\ ,\ \text{Get } N1 \| N2 \text{ and } K'_s = H(N1 \| N2 \| N3)\ ,$$

$$K_s=DP_{KUsms}(EP_{KRsms}(K_s)),\ \text{If } K'_s == K_s \text{ Sender PC(a) can get } K_s$$

Now the user can send mail message M to the receiver using Ks and, at the same time, carry out safe mail transmission process using the authentication/encryption function.

4.3 Sender Authentication and Encryption/Decryption

The sender can get the public key of the receiver to which the mail is to be sent, and its private has already been kept in a safe place. In addition, it is allocated K_s by the SMS server for a specific period of time. Because this process is done using SMS messages, it is safe from attacks such as packet sniffing. The result of hashing the message through H(M) is encrypted using the sender's private key for authentication, and $EP_{KRa}(H(M))$ is joined with the original message $(EP_{KRa}(H(M)) \| M)$. For message encryption, this value is again encrypted using K_s as a session key through the conventional encryption method $((EC_{Ks}(EP_{KRa}(H(M)) \| M))$. However, because the receiver does not know K_s, it encrypts K_s using the public key of the receiver and joins the result with $EC_{Ks}(EP_{KRa}(H(M)) \| M)$ $(EC_{Ks}(EP_{KRa}(H(M)) \| M) \| ER_{KUb}(K_s))$. Lastly, this value is delivered to the receiver.

The receiver knows its own private key and the sender's public key. First, to get K_s, it decrypts $ER_{KUb}(K_s)$ using its own private key. Using K_s obtained through the decryption, the encrypted message is decrypted

$(EC_{Ks}(EP_{KRa}(H(M)) \| M))$. In the decrypted message, $EP_{KRa}(H(M))$ is decrypted using the sender's public key for sender authentication. M, which was joined with the H(M) obtained from the process above, is compared with hashed H(M) and, by doing so, the sender is authenticated. The process above performs procedure similar to existing DomainKey and PGP.

5. Evaluation and Analysis Results

5.1 Safety Evaluation Result on the Proposed Method

In the existing DomainKey method, a mail message to be sent is signed through MTA and sent to the receiver's MTA. At that time, a public key/private key pair should be created in MTA and the receiving MTA should receive the sender's public key and verify it. Thus, the method should be supported by safe key allocation and management structure.

The method proposed in this study encrypts the public key using the public key/private key pair as in existing PGP and DomainKey, so it provides functions for the integrity, confidentiality and authentication of mail messages.

Particularly because the method proposed in this study established a double authentication system that sends key-related values through a wireless mobile phone message in addition to existing TCP/IP-based network traffic using the mobile-phone-based individual verification function in the SMS system, it could provide reinforced email security and sender authentication structure compared to PGP and DomainKey.

Email messages can be monitored using a packet sniffing tool like Ethereal. The method proposed in this study enhanced safety compared to existing methods as it introduced a separate wireless network like a mobile phone rather than using only TCP/IP-based network environment. For session key K_s, it showed a one-way characteristic because it used a hash function like SHA-1 or MD5. Thus, because the safety of K_s is based on the safety of the hash function, the proposed method provides advanced authentication and security functions compared to the existing DomainKey and PGP methods.

5.2 Comparison with existing methods

The model proposed in this study establishes a reinforced security system through double encryption, namely, mail message encryption and sender authentication. In addition, it receives symmetric key Ks for message encryption from the SMS server in a safe way. [Table 1] shows the results of comparing the proposed system with existing ones. The results show that the proposed method is superior to existing ones.

Table1 Comparative Computation about safety and Capability

Feature / Technique	Spam interception	Sender Authentication	Mail Decryption	etc
Filtering[4]	Filtering	×	×	Mail content Filtering
SPF[5]	IP Address	△	×	DNS Search
DomainKey[6]	Sender Authentication	△	◇	Public Key
PGP[7]	No	◇	△	Key Ring
Proposed Method	**Sender Authentication**	**△**	**△**	**Two factor Authentication**

○: A ×: N/A △:good ◇:moderate ▽:bad

6. Conclusions

In order to supplement the unsafe key allocation process of existing methods with key allocation using SMS of mobile phones, the present study proposed a model that delivers the key of public key-based algorithm to the sender and the receiver safely in the processes of message encryption and sender authentication. The safety and security of SMS key allocation have already proved in existing payment systems. In addition, in substitute for existing simple IP comparison and filtering techniques, a sender authentication technique was proposed and, as a result, both sender authentication and mail safety were provided at the same time.

Based on this study, we expect development in various ways through combining the SMS-based double authentication system with the authentication process in mailing systems and Web-based authentication systems.

Acknowledgements

This work is supported by the University IT Research Center(ITRC) Project(IITA-2006-(C1090-0603-0016)).

References

[1]Pam Cocca, "Email Security Threats", SANS Institute 2005, September 20, 2004.

[2]http://en.wilipedia.org/wiki/Simple_Mail_Transfer_Protocol

[3]Wade Trappe, Lawrence C. Washington "Introduction to CRYPTOGRAPHY with Coding Theory", Prentice Hall, 2002.

[4]Nam Tran, "Anti spamming - How to filter unsolicited e-mail on your mail server", December 27 2001.
[5]http://www.openspf.org/
[6]http://antispam.yahoo.com/domainkeys
[7]http://www.pgpi.org/
[8]www.spambreaker.co.kr/loss_expense.html
[9]http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[10]Pret Fisher, "Creating a Hardened Internet SMTP Gateway in Exchange 2003", February 10, 2005.
[11]http://www.joewein.de/sw/spam-challenge-response.htm
[12]http://kr.antispam.yahoo.com/domainkeys
[13]Wade Trappe, Lawrence C. Washington "Introduction to CRYPTOGRAPHY with Coding Theory", Prentice Hall, 2002.

Jong-Won Seo received the B.S. degree in Computer Science from Cheonan University, Korea, in 2006. He is currently a M.S. degree in Computer Information from Hanshin University, Korea. He main research interests are in the areas of network security, Cryptography.

Je-Gyeong Jo received the B.S. degree in Computer Science from Hanshin University, Korea, in 2006. He is currently a M.S. degree in Computer Information from Hanshin University, Korea. He main research interests are in the areas of network security, Software Engineering.

Hyung-Woo Lee received the B.S., M.S. and Ph.D. degrees in Computer Science from Korea University in 1994, 1996 and 1999, respectively. From 1999 to 2002, he was an assistant professor in the Division of Information and Communication Engineering, Cheonan University. He is currently an associate professor in the Division of Computer, Information and Software, Hanshin University, Korea. His research activities are mainly in the areas of information security, network security, and wired/wireless IDS/IPS, Anti-SPAM protocol.