JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 18, No. 7, pp. 1403-1409, Nov. 2017

SMTP와 POP3를 활용한 암호화 메일 프로그램 구현

공 건 웅[1] · 원 용 관[2*]
[1]전남대학교 LG스마트융합공학과
[2]전남대학교 컴퓨터공학부

Implementation of Encrypted Mail Program using SMTP and POP3

Keon-Woong Kong[1] · Yonggwan Won[2*]
[1]Department of LG Smart Convergence Engineering, Chonnam National University, Gwangju, 61186, Korea
[2*]School of Electronics and Computer Engineering, Chonnam National University, Gwangju, 61186, Korea

[요 약]

인터넷이 발달함에 따라 보안의 중요성이 커지고 있다. 그중 전자메일은 이제는 기업과 일반 사용자들이 인터넷에서 사용하는 중요한 서비스 중 하나가 되었다. 그러나 스니핑 공격, 아이디, 패스워드 유출 등 보안 취약점이 생기면서 많은 문제가 되고 있다. 본 논문은 비밀을 요하는 메일 내용을 대칭키 방식으로 암호화하여 별도의 복호화 과정을 수행하지 않는 경우 메일 내용을 읽을 수 없는 암호화 메일 프로그램의 구현 방법을 소개한다. 기존의 메일 서버를 사용하기 위해 SMTP 및 POP3 규약을 준수하고 서버에는 암호화된 메일이 저장되며 복화화는 송신자와 수신자 사이에 미리 공유한 키를 이용하여 수신자 및 송신자의 단말에서만 복화화가 이루어진다. 이러한 방식의 암호화 메일링 방법은 기존의 보안 시스템의 변경 없이 추가적인 보안 장치로 적용이 가능한 효율성이 있다.

[Abstract]

As the Internet evolves, security becomes more important. Especially, e-mail has become one of the most important services that companies and ordinary users use on the Internet. However, security vulnerabilities such as sniffing attacks, IDs, and password spoofs are causing many problems. This paper introduces an example of implementation of encrypted mailing program with which the secured mail is encrypted by symmetric key methode and the encrypted message can not be read without proper decryption. In order to use the current mailing systems, we keep the rules related to SMTP and POP3, and only the encrypted message is stored in the mail server system and the message can be decrypted only at the terminals of the senders and the receivers with the key which is shared in advanced by independent route between them. This implementation scheme can provide an efficiency that it does not request any change of current mailing system, which can be an additional security protection.

색인어 : 메일, SMTP, POP3, 암호화, 복호화
Key word : Decryption, Encryption, Mail, POP3, SMTP

http://dx.doi.org/10.9728/dcs.2017.18.7.1403

Received 21 September 2017; **Revised** 10 October 2017
Accepted 25 November 2017

***Corresponding Author; Yonggwan Won**

Tel: +82-62-530-1804
E-mail: ykwon@jnu.ac.kr

Ⅰ. 서 론

최근 인터넷을 이용한 정보기술의 발달은 정보처리 및 정보교환을 활발하게 하였고 이로 인해 인터넷을 통한 메일의 송수신의 증가를 발생시켰다. 이를 위해인터넷을 통한 중요 내용을 주고받을 경우 안전하고 신뢰할 수 있도록 보안에 관한 많은 방법들이 연구되었다. 그러나 개인정보를 관리하는 서버들의 보안문제로 인해 아이디, 비밀번호 등 개인정보유출이 발생하고 있으며, 다양한 해킹 방법으로 인해 이메일 내용이 원하지 않는 곳에 유출되는 사회적 문제를 야기 시킨다.

이러한 정보의 유출로 인해 송수신 중에 메일 내용을 암호화해주는 기술을 발전시켰으나 사용자의 아이디 및 비밀번호가 노출이 되는 경우 여전히 메일 내용의 유출을 막을 수 없게 된다. 또한, 메일 서버에 로그인 한 채로 잠시 컴퓨터를 떠난 사이 타인이 메일 내용을 훔쳐 볼 수 있는 위험도 존재한다.

본 논문에서는 비밀을 요하는 메일을 대칭키 방식으로 암호화하여 별도의 복호화 과정을 수행하지 않는 경우 메일 내용을 알 수 없도록 구현하는 방법을 속한다. 특히, 암호화된 메일의 내용이 서버에 저장되고 복호화는 사전에 송신자와 수신자 사이에 공유한 키를 이용하여 송신자와 수신자의 단말에서만 복호화가 가능하다. 이러한 방식의 암호화 메일링 방법은 기존의 보안 시스템의 변경 없이 추가적인 보안 장치로 적용이 가능한 효율성이 있다.

Ⅱ. 관련 연구

2-1 SMTP

SMTP(Simple Mail Transfer Protocol)는 TCP/IP (Transmission Control Protocol/Internet Protocol)에서 포트번호 25번을 사용하는 프로토콜이다. 대부분의 메일 송신을 위해 사용하며 상대 서버를 지시하기 위해서 DNS(Domain Name System)의 MX레코드가 사용된다. RFC2821에서 규정되어 사용되고 있으며 메일 서버로의 송수신 뿐만 아니라 메일 클라이언트에서 메일서버로 메일을 보낼 때에도 사용되는 경우가 많다 [1]. SMTP는 텍스트 기반의 프로토콜로서 Require /Response에서 메시지 뿐만 아니라 모든 문자가 7 비트 ASCII(American Standard Code for Information Inter)코드로 되어있어야 된다고 규정되어 있다. 그렇기 때문에 문자 표현에 8비트 이상의 코드를 사용하는 언어나 첨부파일과 자주 사용되는 각종 바이너리는 MIME(Multipurpose Internet Mail Extensions)방식을 통해 아스키코드로 변형된다 [1].

MIME는 기존에 사용하던 아스키 기반의 메시지 형식을 그대로 유지하면서, 메시지 내용에 멀티미디어 데이터 인코딩 방법을 추가로 정의한다는 특징이 있다. 송신측에서는 메일을 전송하기 전에 Non-ASCII 데이터를 ASCII 데이터로 변환해 주어야 하며, 수신측에서는 원래 형식으로 역변환 해야 한다. 그림 1이 이들의 관계를 설명한다 [2].

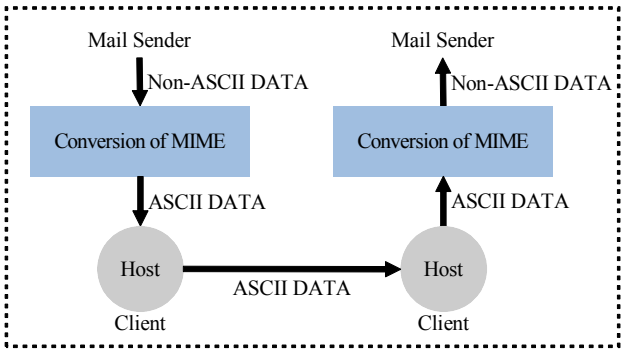

그림 1. MIME 구조
Fig. 1. Structure of MIME

MIME 기능을 사용하여 메일 송신자가 전송하려는 Non-ASCII 형식의 데이터를 미리 ASCII 형식으로 변환한다. 메일 수신자는 반대로 ASCII 형식의 데이터를 원래의 데이터 형식으로 역변환하여 사용자 화면에 보여주는 과정을 거친다 [2]. 결과적으로 인터넷으로 전송되는 모든 메일 데이터는 여전히 ASCII 형식으로 전송된다. MIME에 대한 멀티미디어 데이터의 지원은 송수신자의 양 끝단에서 이루어지는 작업이다 [2].

현재 알려진 대표적인 SMTP 서버로는 현재 가장 많이 사용되는 공개 소프트웨어인 Sendmail, Qmail 등이 있고 사용 메일 서버로 SUN Java System Messaging Server, MS Exchange Server등이 많은 시장을 점유하고 있다 [3]. 그런데 최근 SMTP 서버는 네트워크 서버로서 포트가 모든 네트워크상에 공개되어야 하는 특성 때문에 서버는 직접적인 보안 취약에 노출되고 해커들의 일반적이고 가장 손쉬운 공격 대상이 되고 있다 [4].

이에 따라 인터넷에서는 SMTP를 사용하는 기존의 전자우편 시스템에 메시지 기밀성, 무결성, 송신자 인증, 송신 부인-봉쇄 등의 정보보호 서비스를 제공하기 위하여 PEM(Privacy Enhanced Mail)을 정의하였다 [4]. 그러나 PEM은 인터넷의 각 우편서버간의 메시지 비밀성과 인증만을 다루고 있고, 서버와 클라이언트간의 메시지 비밀성과 사용자 로깅정보의 노출에 대해서는 다루고 있지 않는 실정이다 [4].

2-2 POP3

POP3(Post Office Protocol – Version 3)는 SMTP를 제공하지 못하는 호스트들이 SMTP를 제공하는 워크스테이션을 서버로 사용하여 메일을 처리할 수 있도록 고안된 서비스이다 [5].

즉 POP3는 메일서버에 저장되어 있는 메일을 원하는 시간과 장소에서 가지고 올 수 있는 프로토콜이다. 사용자의 전자메일은 서버의 mailbox에 저장이 된다. POP3클라이언트는 POP3을 이용해서 메일을 읽을 수 있다. 새로운 메일이나 답장은 SMTP를 이용해서 클라이언트로부터 서버에 전달이 된다. 클라이언트로부터 보내어지는 메일은 반드시 POP3 서버를 경

유할 필요는 없으며 메일 수취인이 있는 원격 호스트로 바로 보낼 수도 있다. 대부분의 경우에는 POP3서버가 곧 SMTP서버의 역할을 하게 된다. 왜냐하면 이러한 구성이 시스템 관리를 효율적으로 할 수 있기 때문이다 [6].

초기 값으로 서버 호스트는 POP3 서비스를 제공하기 위해 TCP 포트 110번을 참조하게 된다. 클라이언트가 이 서비스를 이용하기 위해서는 서버 호스트와 이 포트를 통해서 TCP 연결을 이루어야 한다. 연결이 이루어 졌을 때 서버는 접속 메시지를 클라이언트에게 보내게 된다. 그 후에 클라이언트와 서버는 접속이 종료되거나 취소될 때까지 명령어와 그 결과를 서로 주고받게 된다 [6].

2-3 Packet Sniffer

패킷 스니퍼(Packet Sniffer)란 네트워크 또는 네트워크의 일부를 통과하는 통신을 볼 수 있는 소프트웨어 프로그램이다. 데이터 스트림이 네트워크를 오고 갈 때, 이 프로그램이 각 패킷을 포착해서 복호하여 콘텐츠를 분석한다. 네트워크의 고장 수리, 네트워크로의 침투 시도 탐지, 네트워크 사용도 점검 및 의심스러운 콘텐츠 걸러내기, 다른 네트워크 사용자 및 그들의 비밀 번호 수집 시도 탐지 등의 기능을 가지고 있다 [7].

그러나 대부분의 패킷들은 암호화 되어있지 않아 해킹에 노출되기 쉽다. 따라서 네트워크의 중간에서 남의 패킷 정보를 도청하는 해킹유형으로 변경되어 사용된다. 이러한 해킹유형을 스니핑이라 한다.[7]

LAN 상에서 개별 호스트를 구별하기 위한 방법으로 이더넷 인터페이스는 MAC(Media Access Control) 주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC 주소는 서로 다른 값을 갖는다. 따라서 로컬 네트워크상에서 각 각의 호스트는 MAC 주소에 의해 유일하게 구별될 수 있다 [8].

이더넷은 로컬 네트워크 내의 모든 호스트가 같은 선(wire)을 공유하도록 되어 있다. 따라서 같은 네트워크내의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다. 하지만 이더넷을 지나는 모든 트래픽을 받아들이면 관계없는 트래픽까지 처리해야 하므로 효율적이지 못하고 네트워크의 성능도 저하될 수 있다. 그래서 이더넷 인터페이스(LAN 카드)는 자신의 MAC 주소를 갖지 않는 트래픽을 무시하는 필터링 기능을 가지고 있다. 이 필터링 기능은 자신의 MAC 주소를 가진 트래픽만을 보도록 한다 [8].

또한 이더넷 인터페이스에서 모든 트래픽을 볼 수 있도록 하는 기능을 설정할 수도 있는데 이를 'promiscuous mode'라 한다. 스니퍼는 이더넷 인터페이스를 이러한 promiscuous mode로 설정하여 로컬 네트워크를 지나는 모든 트래픽을 도청할 수 있게 된다 [8].

일반적으로 앞서 설명한 스니핑을 방지하는 방법으로 스위칭 허브를 사용하게 된다. 스위칭 허브는 로컬 네트워크를 여러 개의 세크먼트로 나누어 쓸 수 있도록 하는데, 각 세그먼트내의 트래픽은 다른 세그먼트로 전달되지 않는다. 따라서 스위칭 허브를 이용하여 업무별로 또는 독립적인 사이트별로 네트워크를 나누어 놓으면 다른 네트워크 세그먼트 내의 네트워크 트래픽을 도청할 수 없게 된다. 하지만 Switch Jamming, ARP Redirct나 ICMP Redirct 등의 기법을 이용하여 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있는 방법도 있다 [8].

Ⅲ. 암호화 메일 프로그램 구현

3-1 DES 암호화 알고리즘

암호화 시스템은 송신자가(Sender)가 어떤 평문(Plaintext)을 암호화키(k)와 함께 암호기 E(Encryption Algorithm)에 입력하여 암호문(Cliphertext)이 생성된다. 이 암호문을 수신하여 D(Decryption Algorithm)와 복호화키(k)에 입력하여 송신자가 보내고자 했던 평문을 생성한다 [9].

암호시스템의 안정성은 알고리즘 보다 키의 안전성에 영향을 받는다. 대칭키 암호알고리즘은 메시지를 처리하는 형식에 따라, 스트링 암호방법(Stream Cipher)과 블록암호방법(Block Cipher)으로 나뉘고, 키의 특성에 따라 암복호화 키가 같은 대칭형(Symmetric)암호화 알고리즘과 암복호화 키가 다른 비대칭형(Asymmetric) 암호화 알고리즘으로 분류한다 [10].

또한 암호키 분배와 관리방법에 따라 비밀키 암호시스템(Secret Cryptosystem)인 관용키 암호화 시스템과 공개키 암호화 방식(Public Key Cryptosystem)으로 나눈다 [11].

DES(Data Encryption Standard) 알고리즘은 64비트의 블록 암호화 알고리즘으로 56비트 크기의 암호화키로 암호화된다. 따라서 생성 가능한 암호화키는 최대 256(약 7200조)가지이다. 암호화는 하나의 블록인 64비트를 L1(32비트)과 R1(32비트)으로 나눈 뒤, R1을 암호화키로 생성한 S-Box를 통해 f 함수를 만들어 치환한 후 이 값을 L1과 논리합하고, L2와 R2의 위치를 바꾸는 두 가지 기본 변환을 통해 이루어진다 [11].

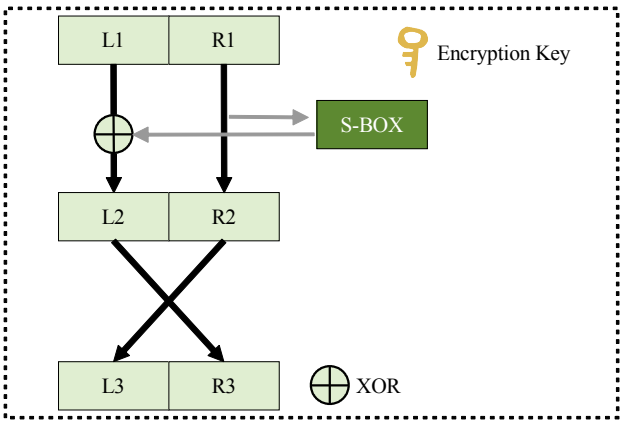

그림 2. DES 암호화 과정
Fig. 2. Procedure of DES Encryption

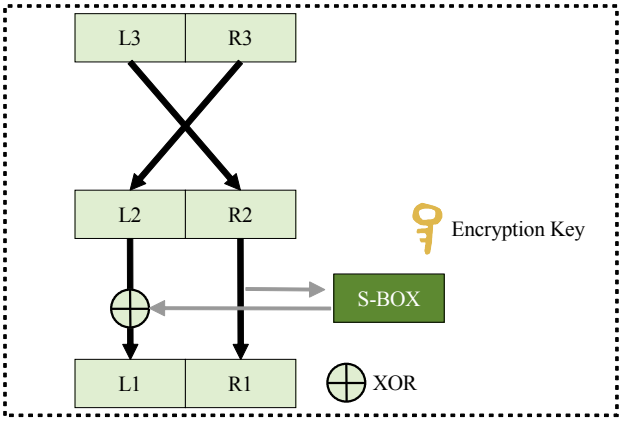

그림 3. DES 복호화 과정
Fig. 3. Procedure of DES Decryption

암호학에서는 암호화 과정의 한 단계를 라운드(Round)라 표현하는데, 혼돈이 바로 라운드 과정에서 이루어진다. DES는 하나의 블록에 대해 이러한 과정을 16번 수행하므로 16라운드 알고리즘이다. 복호화는 그림 3과 같이 암호화의 반대 과정이다 [11].

S-Box란 입력이 6비트 단위이며 출력이 4비트 단위인 S1~S8로 나누어지며 S1~S8을 지나 32비트가 출력된다 [10].

3-2 SMTP와 POP3 클라이언트 프로그램

본 논문에서 제안하고 있는 암호화 메일 송수신 프로그램은 외부 SMTP 및 POP3 서버를 연결하여 메일 송수신 기능을 포함하고 있으며 기존의 메일 시스템을 그대로 사용할 수 있는 장점이 있다. 즉, 자신이 기존에 사용하는 메일서버의 SMTP 및 POP3의 사용 설정을 한 뒤 메일서버의 SSL 유/무, Port 등을 설정하면 기존의 메일시스템을 이용할 수 있다.

그림 5 및 그림 6을 보면 기존의 웹메일(네이버)에서 SMTP와 POP3 서버를 설정하면 기존의 메일시스템과 같이 메일을 수신 및 송신이 가능하다는 점을 보여주고 있다.

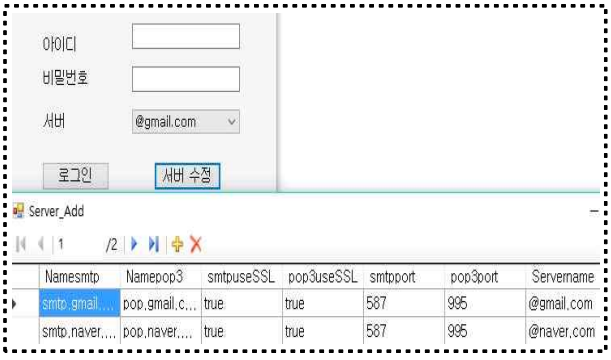

그림 4. 메일 서버 설정 및 로그인 화면
Fig. 4. Sreen of setting mail server and log-in

그림 5. 네이버 메일 편지함 화면
Fig. 5. Screen of Naver mail box

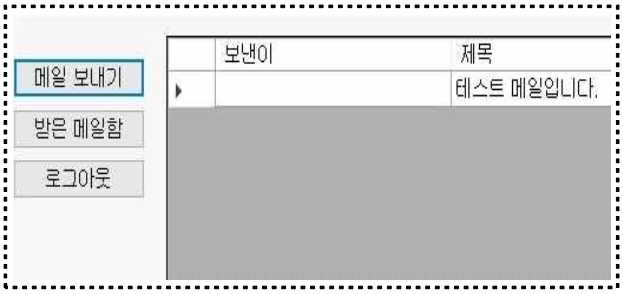

그림 6. 암호화 메일 송수신 프로그램 화면
Fig. 6. Screen of program for encrypted mail

3-3 SMTP와 POP3를 활용한 암호화 메일 송수신 프로그램

제안하는 암호화 메일 송수신 프로그램의 전체구조는 암호화기, SMTP, POP3 클라이언트 부분으로 구성된다. 구조도는 아래 그림 7과 같다.

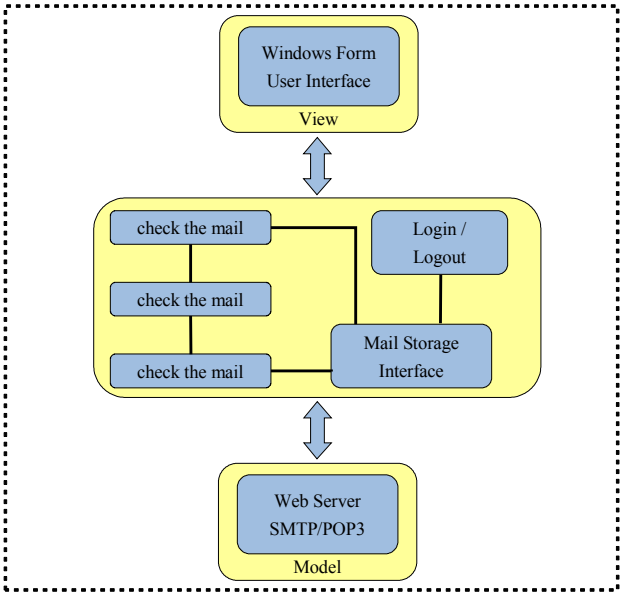

그림 7. 암호화 메일 송수신 프로그램 구조도
Fig. 7. Function diagram of mail sending-receiving program

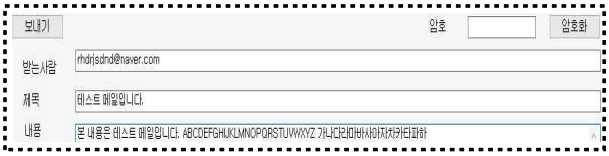

그림 8. 암호화 전 메일내용
Fig. 8. Mail content before encryption

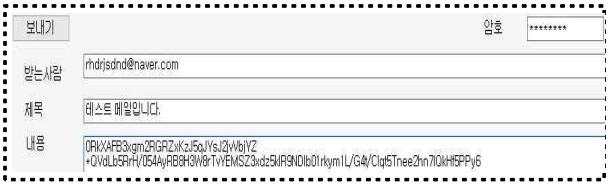

그림 9. 암호화 후 메일내용
Fig. 9. Mail content after encryption

그림 8 및 그림 9에는 암호화 전/후의 메일내용이며 정상적인 메일 내용을 입력한 후 8자리의 암호화 키를 입력하여 암호화를 수행하면 암호화 문구가 생성되며, 이는 클라이언트에서 이루어진다. 암호화된 메일 내용은 '보내기(Send)'를 누르면 수신자에게 메일이 전송되고 그림 10 및 그림11처럼 암호화된 상태로 전송이 완료된다. 그림 11에서 보는 바와 같이 메일 서버에 저장된 메일은 암호화된 상태이다. 즉, 기존 메일서버의 소수신 체계를 그대로 준수하면서 클라이언트 단말에 암호화 및 복화화 기능을 추가하여 서버의 노출에도 안전하게 비밀을 유지할 수 있다.

그림 10. 복호화 전 메일 수신 화면
Fig. 10. Screen of received mail before decryption

그림 11. 메일서버 상의 송신된 메일 내용
Fig. 11. Content of the sent mail in the server

그림 12. 복호화 된 메일 내용
Fig. 12. Content of the decrypted mail

암호화된 메일은 사전에 별도의 방법으로 송신자와 수신자 간에 공유된 키를 입력하여 클라이언트의 '복호화' 기능에 의해 그림 12와 같이 평문으로 복호화된다. 한편, 복호화는 클라이언트 단말에서 실행되므로 서버에는 암호화된 상태로 메일 내용이 남아 있게 된다.

Ⅳ. 결론

인터넷이 발달함에 따라 보안의 중요성이 커지고 있다. 그중 전자메일은 이제는 기업과 일반 사용자들이 인터넷에서 사용하는 가장 중요한 서비스 중 하나가 되었다. 이에 따라 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 스니핑 공격은 웹호스팅, 인터넷 데이터센터(IDC) 등과 같은 여러 업체가 같은 네트워크를 사용하는 경우 특히 문제가 될 수 있다. 하나의 시스템이 공격당하게 되면 그 시스템을 이용하여 네트워크를 도청하게 되고, 다른 시스템의 사용자 ID와 비밀번호를 파악하는 것이 가능하다[12].

또한 메일 서비스를 제공하는 대형포털 사이트의 아이디 및 비밀번호를 해킹하여 가입자의 메일 내용을 훔쳐보는 위험한 상황이 발생할 수 있으며, 메일 서버에 로그인 한 채로 컴퓨터를 잠시 떠난 사이 타인이해 메일을 엿볼 수 있는 위험이 존재한다.

이에 따라 중요한 메일 내용이 존재할 경우 서버에서 많은 보안프로그램이 존재하지만 아이디 및 패스워드가 누출되거나, 스니핑을 통해 직접적인 메일 내용이 탈취되거나, 메일 서버에 로그인 한 채로 잠시 자리를 비워 타인이 훔쳐보기를 하게 되는 경우 메일 내용에 대한 보안을 유지 할 수 없게 된다.

이에 대한 해결 방법으로 본 논문에서 제시하는 SMTP와 POP3를 활용한 암호화 메일 송수신 프로그램은 패킷 스니핑, 아이디, 패스워드 유출 등 보안에 취약한 상황 발생 시 메일 내용을 안전하게 지킬 수 있으며, 타인에 의한 훔쳐보기에도 안전하게 메일 내용을 보호할 수 있을 것이다.

향후 추가적인 개발 과제로는 본 논문에서 제시한 암호화 메일 송수신 프로그램에 첨부 파일에 대한 보호 방법으로 유사한 기법의 암호화 기능을 적용하여 첨부 파일의 보안 취약성을 해결할 수 있을 것이다.

참고문헌

[1] wikipedia, SMTP (Simple Mail Transfer Protocol)[Internet], Available: https://ko.wikipedia.org/
[2] Ki-Hyun Park, Data communication and computer network, Hanbit Academy, 2013.
[3] Young-Jong Kim, "A Distributed Architecture based SMTP Server for Large Email Service", The Journal

of Information Processing Society, Vol. 16-C, No. 5, pp.597-604, 2009.

[4] Jum-Gu Kim, “Design of secure electronic mail system for information protection services”, The Journal of Narnseoul Univ, Vol. 5, pp.84-95, 1999.

[5] Myers, Rose, Post Office Protocol – Version 3, IETF, RFC 1725, 1995

[6] Jong-Hee Kim, “Development of the Secure-POP3 using the Encryption of Account Information”, The Journal of Information Science Society, Vol. 3, No. 6, pp.708-713, 1997.

[7] Korea Information Technology Association, http://www.tta.or.kr/.

[8] Hyun-Mi Park, Network Sniping Technology and Prevention Measures, https://www.linux.co.kr/security/certcc/tr2000-07.htm/.

[9] Gil-Hyun Nam, “A Study on the Crypto-complexity of DES and A Proposal of Extended DES-like Cryptographic Algorithm”, The Journal of Korea Communications Information Society, Vol. 3. No. 2, pp.3-15, Dec 1993.

[10] Ho-Shin Na, Study on comparison of DES and SEED, Master, Dong-guk University, Seoul, 1999.

[11] Dae-Il Yang, Information Security Initiative : Everything You Learn About One Piece Of Security Theory, Hanbit Academy, 2013.

[12] PMG Knowledge engine laboratory, A dictionary of common events, ParkMoonGak.

공건웅(Keon-Woong Kong)

2016년 : 전남대학교 (공학사)
2016년 ~ 현재 : 전남대학교 대학원 (공학석사)

※관심분야 : 지능컴퓨팅(Intelligence Computing), 의공학(Biomedical Engineering), 신호처리(Signal Processing) 등

원용관(Yonggwan Won)

1987년 : 한양대학교 (공학사)
1991년 : 미주리주립대학교 대학원 (공학석사)
1995년 : 미주리주립대학교 대학원 (공학박사)

1995년~1996년: 한국전자통신연구원 선임연구원
1996년~1999년: 케이티 연구개발본부 선임연구원
1999년~현재: 전남대학교 전자컴퓨터공학부 교수
2004년~현재: BIT융합기술사업단장
2014년~현재: 전남대학교 창업보육센터장
※관심분야 : 지능컴퓨팅(Intelligence Computing), 형태인식(Pattern Recognition), 의생명공학(Biomedical Engineering) 등