Journal of the Korea Academia-Industrial cooperation Society
Vol. 12, No. 5 pp. 2346-2352, 2011

DOI: 10.5762/KAIS.2011.12.5.2346

인트라넷 기반의 웹 메일 시스템 구현

신승수[1*], 한군희[2]
[1]동명대학교 정보보호학과, [2]백석대학교 정보통신학부

A Implement of Web-Mail System based on Intranet

Seung-Soo Shin[1*] and Kun-Hee Han[2]
[1]**Dept. of Information Security, College of Information & Communication,**
[2]**Division of Information & Communication Engineering, Baekseok University**

요 약 인트라넷을 사용하는 메일 시스템은 악의적인 서버 관리자 또는 제 3자가 메일을 해킹할 경우 모든 메일 내용이 그대로 노출 된다. 이를 해결하기 위해서 대칭키 암호 알고리즘을 이용한 안전한 인트라넷 메일 암호 프로토콜에 대해서 제안한다. 제안한 프로토콜은 메일 내용을 송·수신하는 쌍방 간의 합의된 세션 키로 암·복호화하기 때문에 악의적인 의도로 메일에 접근했을 경우에도 세션 키가 노출되지 않는 한 메일 내용을 알 수 없다.

Abstract E-mail systems using the intranet is widely exposed to internal threats should an administrator or a third party decides to misuse the information. To solve this problem, we propose a safe intranet email encryption protocol using the symmetrical-key password algorithm. Since the proposed protocol encrypts the data using a pre-agreed session keys between the users, the data will be safe from malignant access attempts provided that the session key is not exposed.

Key Words : SSL, ARIA, Eclipse, Wireshark, CBC-Mode

1. 서 론

정보통신의 발전과 함께 일반적인 통신 수단이었던 메일이 단순한 커뮤니케이션 수단에서 비즈니스와 금융결재, 전자상거래 등과 밀접하게 연관되면서 메일보안의 중요성이 높아지고 있다. 이로 인해 기존 메일 솔루션 업체들과 보안 솔루션 업체들 간의 제휴가 활발히 이루어지고 있으며 특히, 공공기관 및 보안이 필요한 민간 기업을 중심으로 메일 사용 시 정보보안에 대한 요구가 커지고 있다[1].

인터넷이 발전하면서 불법자료를 외부로 유출시키거나 메일 데이터의 원본 수정을 이용한 악의적인 사용도 빈번히 발생하고 있다. 이렇게 메일을 통한 보안문제가 지속적으로 발생하면서 타인에게 문서를 주고 받는 메일에 대한 보안 의식이 또한 강해지고 있다. 이로 인해 공개키 알고리즘을 통해 메일을 암호화 하여 전송하는 웹메일도 개발되고 있다. 기존 웹 메일 서버들은 서버들끼리 주고받는 엑스트라넷 형식이다. 이는 메일이 생성될 시점에 메일 전체에 대한 보안이 적용되어 메일을 발송하는 것이다. 이 방식은 메일 송신자가 메일을 전송하면 메일 전체를 암호화하여 파일 형태로 수신자에게 전송된다. 수신자는 송신자가 보내준 암호를 입력하여야 수신된 메일을 열어 볼 수 있다. 즉, 메일의 본문 전체를 암호화 시켜 발송하는 것이다. 이제 메일은 단순히 메시지를 전달하는 기능에서 보안 기능이 추가되었다. 인터넷 문화의 변화로 간단한 문자는 메신저를 이용하지만 보관이 필요한 자료나 업무가 중요한 자료는 아직 메일을 통하여 전달된다[2].

악의적인 공격자에 의해 전송되는 과정에서 이메일의 내용이 쉽게 노출되거나 수정될 가능성을 무시할 수 없다. 뿐만 아니라 서버 관리자에 의하여 이메일 내용이 그대로 노출이 된다. 1995년 Bacard등은 이메일의 메시지에 대한 기밀성과 인증을 제공하기 위한 PGP (Pretty good Privacy)를 제안하였다[3].

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 11년 03월 25일 수정일 11년 04월 14일 게재확정일 11년 05월 12일

본 논문에서는 기존 웹 메일 시스템과 제안한 메일 암호 시스템에 대하여 각각의 메일에 대한 전송 패킷을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해서 분석하고, 3장에서는 인트라넷 웹 메일을 구현한다. 그리고 4장에서는 분석하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

기존 보안메일이 작성되면서 저장되고, 수신인에게 전달되는 구간을 살펴보면 작성자가 메일을 작성하는 구간, 수신인에게 메일을 전송하는 구간, 발신인이 수신인에게 보낸 메일을 카피하여 보관하는 구간, 수신인이 받은 보안메일을 복호화 하여 읽어 보는 구간으로 보안메일의 각 단계에서 필요한 기술 특성은 다음과 같다[4].

○ 작성자가 메일을 작성하는 구간 :

작성자는 인터넷을 통해서 보안메일 서버에 접속하므로 아무런 보호 장치 없이 메일을 쓰는 것은 해킹의 위험이 따른다. 그러므로 메일의 내용은 한 글자씩 SSL로 암호화하여 올리는데 SSL의 암·복호화는 인터넷브라우저가 자동으로 지원하므로 사용자는 속도가 다소 느려지는 것 외에는 달리 부담을 느끼지 않지만 솔루션 적으로는 보안서버 지원이 되거나 구입해서 설치해야 한다.

○ 수신인에게 메일을 전송하는 구간 :

발신인이 작성한 메일이 수신인의 메일 서버에 도착할 때 까지는 인터넷을 통해서 여러 장치를 거치게 되는데, 모든 메일은 암호화되어 저장되고 전송되어야 한다. 암호화를 하려면 암호화 알고리즘이 있어야 하며, 우리나라에서 가장 많이 사용하는 것은 ARIA, AES256으로 보면 된다. 이 암호 알고리즘이 결정되면 암호화하고 복호화 할 키와 방식을 결정해야 하는데, 보통 PKI 방식과 DRM 방식을 사용하며 키의 사용법은 대칭형과 비대칭형의 두 가지가 있으나 실전에서는 두 가지를 다 같이 사용한다. 경우에 따라 랜덤키나 Mac Address, 혹은 이미지 기술 등 다른 기술과 함께 여러 번 섞어 사용하기도 한다. 최근의 보안메일에서는 웹 메일 방식을 사용하는데 이렇게 하면 발신인과 수신인의 계정이 모두 같은 웹 메일 서버에 있으니 암호화 된 메일이 밖으로 돌아다닐 일은 없어서 전달이 되고 안 되는 문제는 없어진다.

○ 발신인이 수신인에게 보낸 메일의 카피를 보관하는 구간 :

보안메일에서는 발신인이 보낸 원본메일은 발신인의 보낸 메일함에 암호화되어 안전하게 보관되어져 있어야 한다. 그래야 후일에 발송한 메일과 사본에 대한 원본대조, 발신부인방지, 수신부인방지 등 보안메일의 기본기능에 충실히 대처할 수 있기 때문이다. 그러므로 이렇게 암호화되어 보관 중인 메일은 발신인이 본다고 해도 반드시 발신인임을 인증하는 개인키 등 확인 절차를 거친 후에 조회하게 해야 할 것이다.

○ 수신인이 받은 보안메일을 복호화 하여 읽어 보는 구간 :

최근의 보안메일들은 웹 메일 방식이 주종이므로 이 경우 수신인이 보는 메일은 이미 서버에서는 평문으로 올 것임이 분명하고 이것은 위험하다. 그러므로 별도로 그 구간에 대해서 보안서버(SSL)와 같은 조치를 취해야 안전하게 전송될 것이다.

기존 메일 암호시스템을 캡처프로그램인 wireshark를 이용하여 메일을 전송한 다음 그 패킷을 캡처해 분석한 결과 메일의 제목, 받는 사람의 ID, 메일의 내용이 모두 그대로 노출되는 문제점이 발견되었다. 또한, 기존 메일 시스템은 메일 서버관리자나 악의적인 목적을 가진 제 3자에 의해 메일 내용이 그대로 노출되고 있는 문제점을 가지고 있으며, 또한 국내 대부분 포털사이트의 웹 메일이 웜·바이러스 유포, 개인정보 유출, 나아가 컴퓨터를 마비시킬 수도 있는 심각한 취약점들을 가지고 있다. 본 논문에서는 메일의 내용이 악의적인 서버관리 또는 제 3자에게 모두 그대로 노출되는 문제점을 해결하고자 새로운 인트라넷 메일 시스템을 구현한다. 다음 장에서는 이러한 사항을 고려한 메일 시스템을 구현하고자 한다.

3. 메일 시스템 구현

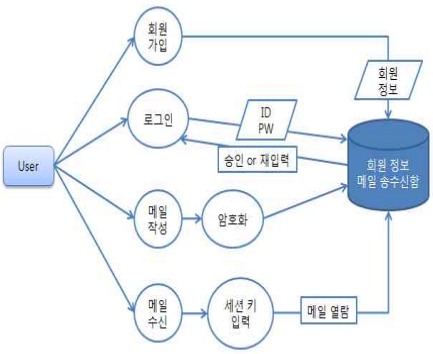
관련 인트라넷 메일 시스템에서 제시된 문제점을 해결하기 위해 본 장에서는 새로운 인트라넷 메일 암호 시스템을 효율적으로 구현하고, 암호모듈 세 가지인 CBC 모드, MD5 해시함수, ARIA 암호 알고리즘을 사용하여 설계된 프로토콜을 Eclipse 프로그램을 사용하여 구현한다[6-13].

3.1 개발환경

제안한 인트라넷 메일 암호 시스템을 구현하기 위해서 O/S, Processor, CPU, RAM, 개발언어, 개발도구, D/B 등의 개발환경은 다음과 같다. O/S는 Window XP SP3를 사용하였고, Process는 Intel(R) Pentium(R)4, CPU는 CPU 3.0GHz, RAM는 1.0GB RAM, 개발언어는 JAVA Programing, 개발도구는 Eclipse, D/B는 MS SQL 2005를 각각 사용하였다.

3.2 시스템 동작 과정

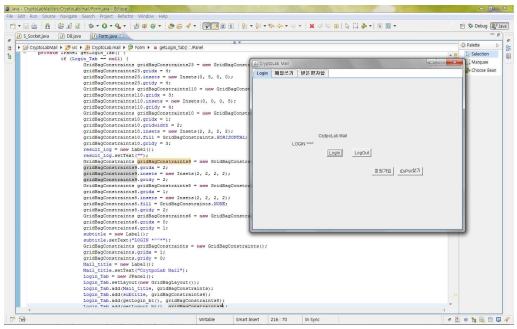
사용자는 메일을 이용하기 위해서 서버에 회원가입을 하게 되고, 회원가입 시 입력된 회원정보들은 개인정보가 유출될 경우에도 제3자가 알아내지 못하도록 해시 함수를 적용한 해시 값을 서버의 회원정보 테이블에 저장된다. 회원 가입을 한 다음, 사용자가 로그인 시, ID/PW를 입력하면 서버는 회원정보 테이블에 저장된 회원정보와 입력된 정보를 비교하여 사용자에 대해서 승인하거나 또는 재입력을 요청한다. 로그인이 승인된 사용자는 메일을 작성하고 송신할 때 ARIA 암호 알고리즘을 통해 메일 내용을 암호화 하여 전송하게 된다. 마지막으로, 메일 수신시에는 송신자와 교환한 세션 키를 통해 키 값을 입력하게 되면 메일 내용을 복호화하여 열람할 수 있다. 이와 같은 메일 시스템 동작 과정은 그림 1과 같다.



[그림 1] 메일 시스템 동작 과정

3.3 프로토콜 구현

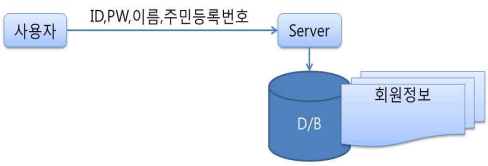
서버에 저장된 메일을 서버관리자나 제3자가 악의적인 목적을 가지고 메일을 열람할 경우 메일의 내용을 송·수신자 외에는 볼 수 없도록 하기 위해서 김희정등[5]이 제안한 프로토콜을 Eclipse 프로그램을 통해서 구현한다. 프로토콜의 구현 단계는 등록 단계, 로그인 단계, 메일 송신 단계, 메일 수신 단계, ID/PW 찾기 단계로 구성된다. 메일 암호시스템에 사용되는 LOGIN-MAIN form에는 Login, Logout, 회원가입, ID/PW 찾기 등으로 구성된다. LOGIN-MAIN form은 그림 2와 같다.



[그림 2] LOGIN-MAIN form

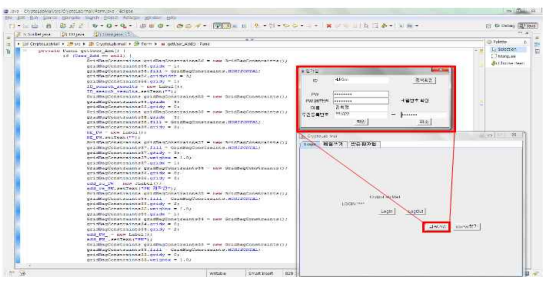
3.3.1 등록 단계

등록 단계는 메일을 사용하기 위해 사용자 Alice와 Bob는 ID, PW, 이름, 주민등록번호를 회원등록 창에 입력한다. 회원 정보는 개인 정보보호를 위해 사용자 Alice와 Bob의 개인정보를 MD5 해시 함수를 사용하여 얻은 해시 값을 Server의 사용자 Alice와 Bob의 테이블에 저장한다. 그림 3은 사용자 Alice와 Bob의 등록 단계 구현과정을 나타낸 것이다.



[그림 3] 등록 단계 구현 과정

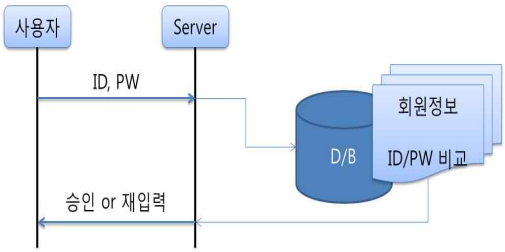
그림 4는 사용자 Alice와 Bob의 등록 단계를 JAVA Programing으로 구현한 실행화면이다.



[그림 4] 등록 단계 폼

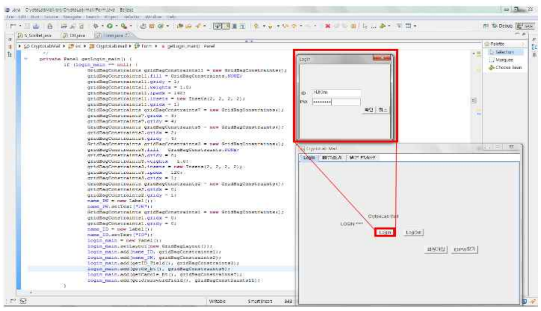
3.3.2 로그인 단계

Alice와 Bob는 메일을 송·수신하기 위해서는 먼저 로그인을 해야 한다. 로그인을 하기 위해서는 사용자 Alice와 Bob가 등록 단계에서 사용했던 ID와 PW를 입력하고, 메일 서버의 D/B는 등록 단계에서 받았던 회원정보 ID와 PW와 사용자 Alice와 Bob가 입력했던 ID와 PW를 비교하여 사용자 Alice와 Bob의 접속을 승인하거나 또는 재입력을 요구한다. 그림 5는 사용자 Alice와 Bob의 로그인 단계의 구현과정을 나타낸 것이다.



[그림 5] 로그인 단계 구현 과정

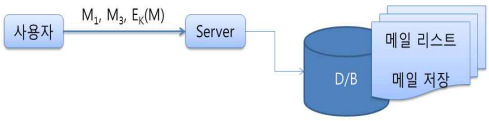
그림 6은 사용자 Alice와 Bob의 로그인 단계를 JAVA Programing으로 구현한 실행화면이다.



[그림 6] 로그인 단계 폼

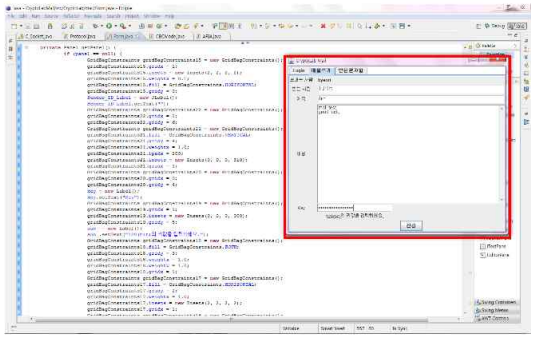
3.3.3 메일 송신

메일을 송신하기 위해서 송신자 Alice는 다음과 같은 정보, 즉, 받는 사람(Bob), 보내는 사람(Alice), 제목, 내용, 키 값을 입력을 하고 나서 메일을 전송한다. 메일 서버의 D/B는 송신자인 Alice에게 받은 메일 리스트와 메일을 서버의 DB에 저장하게 된다. 그림 7은 사용자 Alice가 Bob에게 메일 송신의 구현 과정을 나타낸 것이다.



[그림 7] 메일 송신 구현 과정

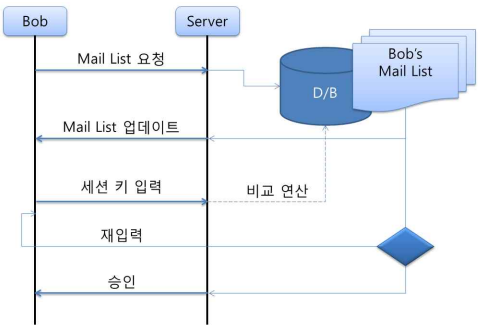
그림 8은 사용자 Alice가 Bob에게 메일 송신 단계를 JAVA Programing으로 구현한 실행화면이다.



[그림 8] 메일 송신 폼

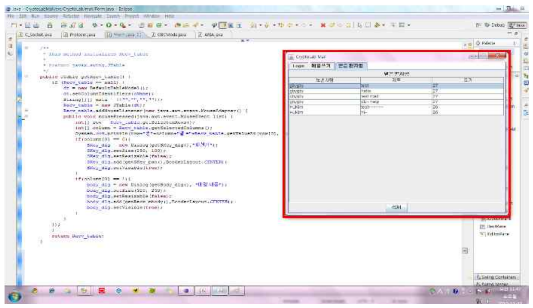
3.3.4 메일 수신

Alice로부터 송신 메일을 수신한 Bob은 수신 된 메일을 열람하기 위해서 Bob가 메일 서버에게 메일 리스트를 요청한다. 메일 서버는 D/B에 저장되어 있는 수신자 Bob의 메일 리스트를 수신자 Bob에게 업데이트 해주고, 수신자 Bob는 송신자 Alice와 교환한 세션 키를 열람하고자 하는 메일 제목을 클릭하여 입력한다. 수신자 Bob가 세션 키를 입력하면 메일 서버는 비교 연산을 하여 일치할 경우 승인, 불일치할 경우 재입력의 메시지를 보낸다. 그림 9는 사용자 Bob이 메일 수신의 구현 과정을 나타낸 것이다.



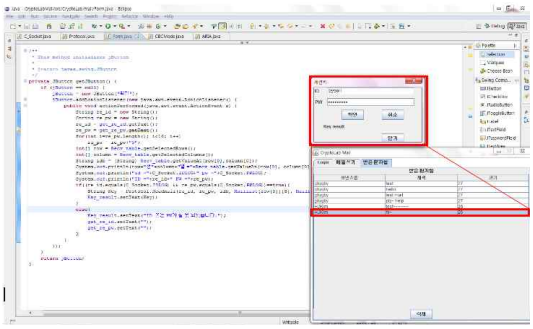
[그림 9] 메일 수신 구현 과정

그림 10은 수신된 메일 목록이 나타나는 메일 수신 단계를 JAVA Programing으로 구현한 실행화면이다.



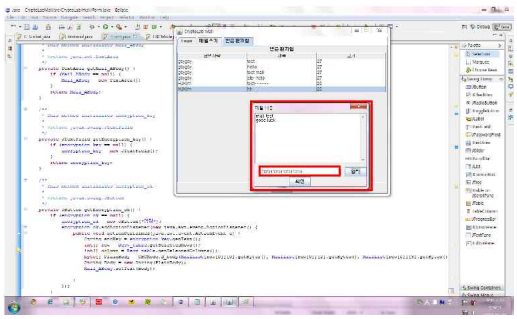
[그림 10] 받은 편지함 폼

먼저, 수신된 메일을 열람하기 위해서는 수신자 Bob와 송신자 Alice간의 교환한 세션 키를 확인해야 한다. 그림 11는 수신된 메일을 선택하여 세션 키 입력 단계를 JAVA Programing으로 구현한 실행화면이다.



[그림 11] 교환한 세션 키 확인 폼

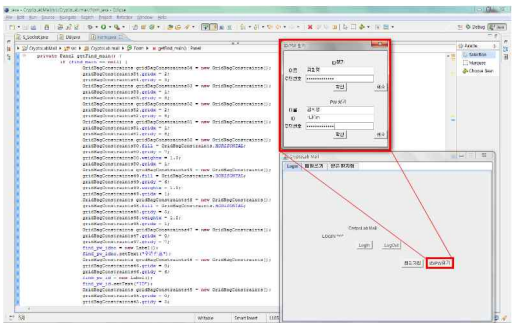
마지막으로 세션 키를 입력한 후 암호화된 메일을 복호화 하면 메일을 열람할 수 있다. 그림 12는 세션 키를 입력하여 메일을 복호화한 단계를 JAVA Programing으로 구현한 실행화면이다.



[그림 12] 세션 키 입력 후 메일 수신 폼

3.3.5 ID/PW 찾기

ID/PW가 기억이 나지 않을 때에는 ID/PW 찾기를 이용해 사용자 Alice와 Bob의 ID/PW를 찾거나, 혹은 임시 PW를 발급 받을 수도 있다. 이때, ID는 이름, 주민등록번호를 이용하여 찾을 수 있고, PW는 이름, ID, 주민등록번호를 이용하여 찾을 수 있다. 그림 13은 ID/PW 찾기를 JAVA Programing으로 구현한 실행화면이다.

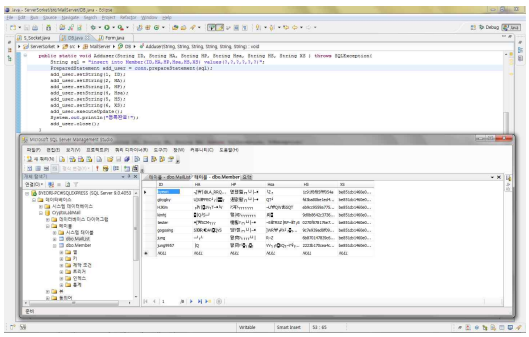


[그림 13] ID/PW 찾기 폼

3.4 DB 테이블

3.4.1 회원정보 테이블

등록 단계에서 입력된 개인정보는 해시 값으로 서버의 회원정보 테이블(DB)에 저장된다. 기존 웹 메일 시스템에서는 입력된 개인정보가 그대로 저장되는데, 메일 암호 시스템에서는 개인정보를 암호화하여 개인정보 유출이란 문제점을 보완하였다. 회원정보 테이블 목록에는 ID, $H_A=h(PW_A \oplus r_A)$, $H_P=(ID\_no \oplus Name)$, $H_{SA}=h(ID_A \oplus x_s) \oplus h(PW_A \oplus r_A)$이 있다. 그림 14은 JAVA Programing으로 구현한 회원정보 테이블이다.

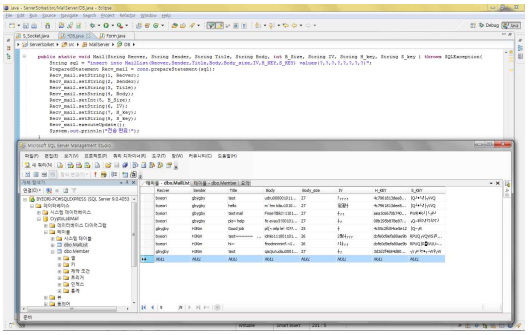


[그림 14] 회원정보 테이블

3.4.2 받은 메일함, 보낸 메일함 테이블

사용자 Alice와 Bob이 전송받은 메일을 DB와 연동하

여 테이블 형식으로 볼 수 있도록 한다. 받은 메일함과 보낸 메일함의 테이블 목록에는 순번, 보내는(받는)사람의 이메일 주소, 제목, 확인, 날짜 및 시간, 메일의 크기 등이 있다. 그림 15는 받은 메일함, 보낸 메일함을 JAVA Programing으로 구현한 실행화면이다.

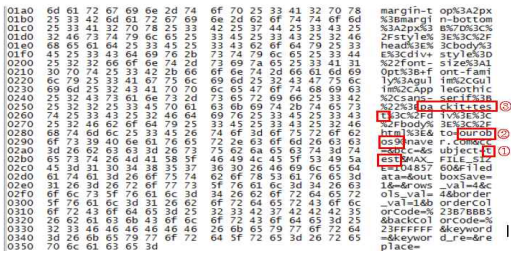


[그림 15] 받은 편지함, 보낸 편지함 테이블

4. 분석

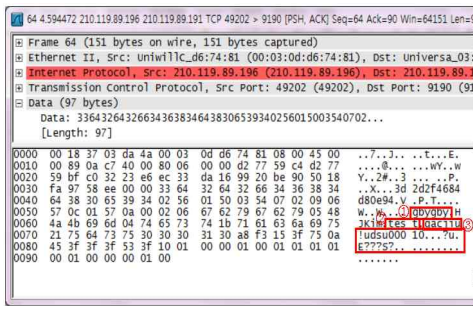
본 논문에서는 기존 인트라넷 메일 시스템과 제안한 메일 암호 시스템에 대하여 각각의 메일에 대한 전송 패킷을 분석한다. 그림 16은 기존 인트라넷 메일 시스템의 메일 전송 내용과 패킷을 캡처한 것이다. 그리고 그림 17는 제안한 인트라넷 메일 암호 시스템에 대한 메일 전송 내용과 패킷을 캡처한 것이다. 먼저, 인트라넷 메일 시스템의 메일을 전송하는 과정의 패킷을 분석한다.

캡처프로그램인 wireshark를 이용하여 기존 인트라넷 메일 시스템에서 메일을 전송한 다음 그 패킷을 캡처해 분석한 결과 그림 16에서 같이 ①메일의 제목, ②받는 사람의 ID, ③메일의 내용이 모두 그대로 노출되는 문제점이 발견되었다.



[그림 16] 기존 인트라넷 메일 시스템의 패킷 캡처

3장에서 제안한 방법을 적용하여 위와 동일한 방법으로 메일을 전송하고 그 패킷을 캡처하여 분석하였다. 캡처프로그램인 wireshark를 이용하여 인트라넷 메일 암호 시스템에서 메일을 전송할 때, 그 패킷을 캡처하여 분석한 결과, 그림 17과 같이 ①받는 사람의 ID, ②메일의 제목은 노출되었지만, ③메일의 내용은 암호화되어 메일의 본문 내용이 노출되지 않았다.



[그림 17] 제안 암호시스템의 패킷 캡처

기존 웹 메일 시스템에서는 메일의 제목, 받는 사람의 ID, 메일의 내용이 그대로 노출되는 문제점이 발견되었다. 이러한 문제점을 해결하기 위해서 제안한 메일 암호 시스템에서는 메일의 내용을 암호화하여 전송하기 때문에 캡처프로그램인 wireshark을 사용하여 통신상에서 메일 패킷을 분석한 결과 메일 내용이 그대로 노출되지 않는다. 이처럼, 메일 암호 시스템은 메일 전송 시에 메일의 내용이 노출되지 않기 때문에 앞에서 분석한 결과를 바탕으로 기존의 웹 메일 시스템보다 안전성이나 효율성이 더 높다고 할 수 있다.

5. 결 론

메일은 인터넷을 통해 누릴 수 있는 가장 오래된 서비스 중 하나이며, 가장 보편적인 수단이다. 기존 메일 시스템은 메시지를 암호화하지 않고 보내기 때문에 송·수신자 이외에 제 3자가 악의적인 의도로 메일 시스템에 접근하여 메일 내용을 모두 볼 수 있다는 문제점을 안고 있다. 향후 정보통신이 발전함에 따라 이러한 피해는 더욱 늘어날 것이다. 이러한 문제점을 해결하기 위해서 메시지를 암·복호화 하여 송·수신한다.

본 논문에서 제안한 메일 암호시스템은 메일을 송·수신할 경우 메일 내용을 암·복호화 하여 송·수신자 외에는 그 내용을 알 수 없도록 한다. 안전한 암·복호화를 위해 송·수신자는 세션 키를 교환하게 된다. 이 세션 키를 입력

해야만 암호화된 메일은 복호화가 되며, 세션 키는 송·수신자 외에는 알 수 없도록 한다.

기존 메일 시스템은 서버관리자가 메일 내용을 볼 수 있었지만 암·복호화를 적용하여 서버는 메일을 저장해주는 역할만 할 뿐, 메일 내용은 볼 수 없도록 ARIA 암호알고리즘으로 암·복호화하여 안전성을 강화하였다. 또한, 연산량이 적어 계산이 빠른 XOR 연산을 사용하였다. 기존 메일 시스템보다 편리성과 접근성은 조금 떨어지지만 무엇보다 안전하다는 장점을 가진다. 이러한 메일 암호시스템은 인트라넷 망에서 사용 가능하며 공공기관 뿐만 아니라 민간기업, 그리고 일반인들에게도 유용하게 사용될 것이다.

참고문헌

[1] 이현수, 박종환, 이동훈, “다중 수신자 환경에서 키워드 검색 가능한 공개키 암호시스템”, 정보보호학회논문지, 제19권, 제2호, pp. 31-37, 2009, 4.

[2] 이성재, “보안메일을 사용해야 하는 이유” http://blog.daum.net/sungji-ses/5627980M, 2007.

[3] A. Bacard, The Computer Privacy Handbook: A Practical Guide to EMail Encryption, Data Protection, and PGP Privacy Software, Peachpit Press, Jan. 1995.

[4] 이시영, 고정국, “보안기능이 강화된 웹 메일 시스템의 설계 및 구현”, 동명대학교 학사논문, 2001.

[5] 김희정, 구본열, 신승수, 한군희, “ ARIA를 이용한 메일 암호시스템에 관한 연구”, 한국산학기술학회 춘계학술발표논문집, pp.77-80, 2010.

[6] 고일석, “예제로 배우는 JAVA Programing”, 혜지원, 2000.

[7] http://www.perfect.sunchon.ac.kr/user/java2_v1.4.0/

[8] 홍성용, “이클립스 기반 JAVA Programming”, 내하출판사, 2008.

[9] 김형준, 손태식, “Java를 이용한 암호학”, 홍릉과학출판사, 2004.

[10] 김도형, “이클립스로 배우는 JAVA Programming”, 삼양미디어, 2010.

[11] 오크스, 스콧, “자바 시큐리티 프로그래밍”, 한빛미디어, 2001.

[12] 최영관, “소설 같은 자바 Third Edition”, 자북, 2008.

[13] 윤선정, 박희숙, 임충재, “MS-SQL Server 구축과 활용”, 이한출판사, 2005.

신 승 수(Seung-Soo Shin) [정회원]

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 정보보호학과 교수

<관심분야>
암호프로토콜, 네트워크 보안, USN, 스마트 카드,

한 군 희(Kun-Hee Han) [종신회원]

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
암호프로토콜, 네트워크 보안, 영상처리