ARIA를 이용한 메일 암호시스템에 관한 연구

김희정*, 구본열*, 신승수*, 한군희**
*동명대학교 정보보호학과, **백석대학교 정보통신학부
e-mail:jung9957@naver.com

A Study on Mail Cryptography System using the ARIA

Hee-Jung Kim*, Bon-Yeol Gu*, Seung-Su Sin*, Kun-Hee Han**
*Dept. of Information Security, Tongmyeung University
**Division of Information & Communication Engineering, Baekseok University

요 약

일반적인 메일 시스템은 제 3자의 악의적인 목적으로 메일의 내용을 열람했을 경우 모든 내용이 그대로 노출 된다는 위험성을 내포하고 있다. 이러한 문제점을 해결하기 위해서, 본 논문에서는 ARIA를 이용한 메일 암호시스템을 제안한다. 제안한 암호시스템은 메일 내용을 송·수신 하는 쌍방 간의 합의된 비밀 키로 암·복호화하여 악의적인 의도로 메일에 접근했을 경우에도 비밀 키가 노출되지 않는 한 메일 내용을 알 수 없도록 설계하였다.

1. 서론

인터넷이 발전하면서 메일 보안에 관한 중요성이 강조되고 있다. 메일은 단순한 커뮤니케이션 수단에서 비즈니스, 금융결재, 그리고 전자상거래 등과 밀접하게 연관되면서 중요성이 커지고 있고 특히 공공기관, 민간기업, 그리고 일반인을 중심으로 메일 사용 시 정보보안에 대한 중요성이 날로 요구되고 있다[1].

메일 사용 시 제 3자의 악의적인 목적으로인한 불법자료 유출과 메일 데이터의 원본 수정을 이용한 악의적인 사용이 빈번히 발생하고 있다. 위와 같은 보안문제가 발생하면서 타인에게 내부 문서를 주고받는 메일에 대한 보안 의식 또한 강해지고 있다[2]. 대부분의 국내 기업용 메일서버들은 이런 암호화에 대한 고려가 없는 경우가 많다. 최근 메일에 대한 동향을 보면 보안 문제가 큰 이슈로 부각되고 있으며 웹사이트 해킹이나 내부 정보 해킹이 큰 문제가 되고 있다[2].

기존 메일 시스템은 제 3자가 악의적인 목적으로 메일의 내용을 열람했을 경우 모든 내용이 그대로 노출이 된다. 이러한 문제점을 해결하기 위해 송·수신자가 세션 키를 교환하고 메일의 내용을 암·복호화 하여 전송하게 된다. 세션 키가 노출되지 않는 한 메일의 내용을 알 수 없도록 ARIA를 이용하여 메일 암호시스템을 제안하였다.

본 논문의 구성은 다음과 같다. 제 2장에서는 연구 동향에 대해 살펴보고, 제 3장에서는 메일 암호시스템의 설계 및 분석을 한 후, 제 4장에서 결론을 맺는다.

2. 연구 동향

2.1. 기존 메일 시스템의 취약성 분석

기존 메일 시스템은 외부의 불특정 침입자로부터 쉽게 ID/Password를 해킹당하고 유출된 ID/Password를 이용하여 마치 자신인 것처럼 정식으로 로그인하여 메일을 열람한다. 또한 메일 시스템을 해킹하여 편지를 통째로 퍼 가가는 경우도 있다. ID/Password를 해킹당하지 않도록 해야 한다[3].

2.2. 메일 암호시스템이 갖춰야할 기본 요건

보안 메일에도 여러 가지 종류가 있고, 그 방법과 성능이 다르므로 구체적으로 따져봐야 한다. 보안 메일이 갖춰야 할 기본 요건은 다음과 같다.

○ 편지의 전달 보장

일반적인 보안 메일의 서버들은 암호화 한 편지를 직접 수신인의 편지함으로 전달하려고 했다. 그러나 실제로는 암호화된 편지가 외부로 나가는 대

신, 스스로 수신인의 계정을 만들어서 거기에 전달해 놓고 수신인에게 어디로 와서 편지를 확인하라는 일반적인 안내 메일을 대신 발송하는 방식이 사용되고 있다[3].

○ 복호화 키의 전달 보장

수신인이 암호화 된 편지를 복호화하려면, 복호화에 사용할 키를 가지고 있어야 한다. 보안메일은 그 키를 Outlook Express에 담아서 보내었는데, 일부 메일 서버들은 복호화용 키를 전달받을 수 없었다. 최근의 보안메일은 이 방법 대신 개인키를 안내 메일에 첨부파일로 보냄으로서 이 문제를 해결하고 있다[3].

○ 보안성과 편의성

공개키 기반의 가장 확실한 인증 방법은 사용자 인증 방식이지만, 1:1 사용을 전제로 하였기에 사용이 제한적이고 까다롭다. 그러므로 사용 목적에 따라서 엄격한 보안을 요구하는 경우는 원칙을 철저히 준수하되, 약간의 융통성을 둬서 편의성을 더욱 강조할 수 있어야 한다[3].

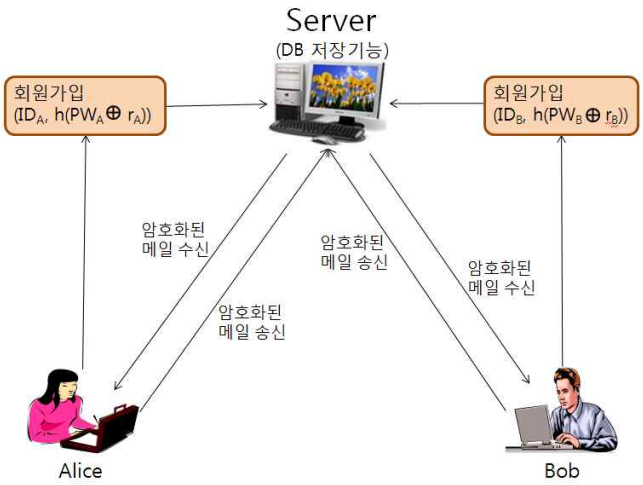
○ 포털사이트용과 기업/조직 용 보안메일

기업이나 조직의 입장에서 보면 누가 어떤 메일을 만들어서 누구에게 보내는지 모든 내용을 감시할 수 있어야 하므로, 보안 관리자의 특별한 역할이 있어야 한다. 즉, 포털사이트용 보안메일은 개인용도이므로 철저히 송·수신자 외에는 아무도 메일을 볼 수 없는 것이면 되지만, 회사/조직용은 보안 관리자가 반드시 내용을 볼 수 있는 구조이면서 여러 가지 문서보안관리 내용들이 함께 하여야 한다[3].

3. 메일 암호시스템 설계 및 분석

3.1. 메일 암호시스템 구성도

기존 메일 암호시스템은 제 3자의 악의적인 공격으로 인해 메일 내용이 그대로 노출된다는 문제점을 갖고 있다. 이러한 문제점을 해결하기 위해 세션키를 이용하여 안전하게 메일을 송·수신할 수 있는 메일 암호시스템을 설계한다. 메일 암호시스템의 전체 구성도는 [그림 1]과 같다.



[그림 1] 메일 암호시스템 구성도

3.2. 암호 모듈

본 논문에서는 CBC 모드, MD5, ARIA와 같은 암호 알고리즘을 사용한다.

○ CBC 모드

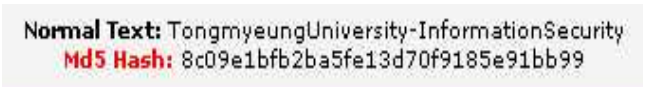
CBC(Cipher Block Chaining:암호문 블록 연쇄) 모드는 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름이다. CBC 모드에서는 1단계 앞에서 나온 출력된 결과를 다음 단계의 암호문 블록과 평문 블록을 XOR 연산을 하여 암호화를 수행한다[4]. [그림 2]는 메시지의 첫 번째 블록을 CBC 모드를 실행시킨 결과이다.

[그림 2] CBC 모드 실행결과

○ MD5 해시 함수

MD5(Message-Digest algorithm 5)는 임의의 길이의 메시지를 입력받아, 128비트의 고정 길이로 출력하는 암호화 해시 함수이다[5]. “동명대학

교 정보보호"라는 메시지를 MD5로 해시한 결과는 [그림 3]과 같다[6].



[그림 3] MD5 해시 함수

○ ARIA 암호 알고리즘

ARIA 암호 알고리즘의 기본구조는 Involution SPN 구조이며, 입출력 크기는 128비트, 키 크기는 128/192/256 비트, 라운드 키 크기는 128 비트, 라운드 수는 12, 14, 16 라운드로 구성된다[7]. "ARIA test mode"라는 메시지를 ARIA 암호 알고리즘으로 실행한 결과는 [그림 4]와 같다.

[그림 4] ARIA 암호 알고리즘

3.3. 메일 암호시스템

메일 암호시스템은 회원가입, 로그인, 세션 키 교환, 메일 송신, 메일 수신의 순서로 이루어진다. 본 논문에서 사용할 기호는 [표 1]과 같다.

[표 1] 표기법

기호	설명
ID_A, ID_B	Alice, Bob의 아이디
PW_A, PW_B	Alice, Bob의 패스워드
E_A, E_B	Alice, Bob의 E-Mail 주소
N_A, r_A	임의의 난수
x_s	서버의 개인키
K_{AB}	Alice가 Bob에게 보내는 암·복호화 키
h( )	해시함수 연산
⊕	배타적 논리합

3.3.1. 회원가입

Alice가 Server에 회원가입을 하는 절차는 다음과 같다.

① 난수 r_A를 선택하여 $h(PW_A \oplus r_A)$와 ID를 Server에게 보낸다.

② Server는 Alice로부터 받은 정보를 이용해 $H_{SA}=h(ID_A \oplus x_s) \oplus h(PW_A \oplus r_A)$를 계산한 값과 $H_A=h(PW_A \oplus r_A)$를 DB에 저장한다.

③ Server는 Alice에게 H_{SA}를 보낸다.

④ Alice는 H_{SA}를 저장한다.

3.3.2. 로그인

Alice는 ID와 PW를 입력하여 로그인을 하게 되면 Server는 DB에 저장된 데이터와 ID_A, $h(PW_A \oplus r_A)$ 값을 비교하여 같을 경우 로그인이 승인이 되고, 같지 않을 경우 로그인이 승인되지 않는다. 로그인 단계는 다음과 같다.

① Alice가 ID_A, $h(PW_A \oplus r_A)$를 입력하고 Server로부터 받은 정보 $H_{SA} \oplus h(PW_A \oplus r_A)$와 난수 N_A를 서버에게 전송한다. 즉, ID_A, N_A, $h(H_A \oplus N_A)$를 전송한다.

② Server는 Alice로부터 받은 정보를 이용해서 $h(H_{SA} \oplus N_A) \stackrel{?}{=} h(H_A \oplus N_A)$를 비교하여 같으면 로그인을 승인하고 다를 경우 재 로그인을 요청한다.

3.3.3. 세션 키 교환 과정

Alice와 Bob은 암호화된 메일을 송·수신하기 위해 세션 키를 교환한다. 안전한 세션 키 교환을 위한 과정은 다음과 같다.

① Alice는 $h(PW_A \oplus r_A)$, N_A와 Bob의 ID_B를 이용하여 $h(H_A \oplus N_A \oplus ID_B)$를 계산하고, 메시지 M_1을 Server에게 전송한다. 즉, $M_1=\{N_A, ID_A, ID_B, h(H_A \oplus N_A \oplus ID_B)\}$이다.

② Server는 DB에 저장된 Alice의 정보를 이용하여 $H_{SA} \oplus h(ID_A \oplus x_s)$, $h'(PW_A \oplus r_A)$를 계산한다. M_1속에 들어있는 정보 N_A, ID_B를 이용하여 $h(H_A \oplus N_A \oplus ID_B)$와 같은지를 비교하여 Alice를 인증한다.

③ Server는 Bob의 정보 $H_B=h(PW_B \oplus r_B)$, $H_{SB}=h(ID_B \oplus x_s) \oplus h(PW_B \oplus r_B)$가 포함된 메시지 M_2를 Alice에게 전송한다. 즉, $M_2=\{N_A, ID_A, H_{SB}, h(H_A \oplus N_A \oplus ID_A \oplus ID_B) \oplus h(H_A \oplus H_{SA})\}$이다.

④ Alice는 Server로부터 받은 정보와 $M_2=\{N_A, ID_A, H_{SB}, h(H_A \oplus N_A \oplus ID_A \oplus ID_B) \oplus h(H_A \oplus H_{SA})\}$를 이용하여 M_2에 포함되어 있는 해시 함수가 같은지를 검증한다. Alice는 Bob과 메시지를 암.복호화 하기 위한 정보를 M_3정보에 포함시켜 M_1, M_3, $E_{K_{AB}}(M)$를 Bob에게 전송한다. 즉,

M_3={ID_A, h(K_{AB}), h($H_A \oplus N_A \oplus ID_A \oplus ID_B$)$\oplus K_{AB}$} 이다.

⑤ Bob은 등록단계에서 생성한 r_A, H_{SA}, H_B를 이용하여 세션키를 추출해 내고 h(K)와 같은지를 검증한다.

3.3.4. 메일 송신

메일을 송신하는 절차는 다음과 같다.

① Alice가 Bob에게 메일을 작성한다.

② ARIA 암호를 이용해 메시지를 세션키로 암호화한다. 즉, $E_{K_{AB}}(M)$이다.

③ Alice는 암호화된 메일과 M_1, M_3, $E_{K_{AB}}(M)$를 Bob에게 송신한다.

3.3.5. 메일 수신

수신한 정보 M_1, M_3, $E_{K_{AB}}(M)$를 통해 정상적으로 복호화를 하게 되면 메일을 확인할 수 있다.

① Alice로부터 온 메일을 확인한다.

② 수신한 정보 M_1, M_3, $E_{K_{AB}}(M)$는 메일을 복호화하기 위해 사용한다.

③ Alice가 보낸 메일을 확인한 다음, 이미 확인했던 메일을 다시 확인하기 위해서는 h($PW_B \oplus E_A$) 값을 다시 입력한다.

3.4. 분석

기존 메일 시스템은 송·수신자 이외에 제 3자에 의해 공격당했을 경우 메일 내용이 그대로 노출되었다. 이러한 문제점을 해결하기 위해 세션키를 이용하여 안전하게 메일을 송·수신할 수 있는 메일 암호 시스템을 설계한다. 메일 수신자는 세션 키를 통해 메일 내용을 복호화하여 메시지를 확인한다. 따라서, 본 논문에서 제안한 ARIA를 이용한 메일 암호 시스템을 적용할 경우 제 3자에 의해서 메시지가 노출이 되지 않는다.

4. 결론

메일은 인터넷을 통해 누릴 수 있는 가장 오래된 서비스 중 하나이며, 가장 보편적인 수단이다[8]. 기존 메일 시스템은 메시지를 암호화하지 않고 보내기 때문에 송·수신자 외에 제 3자가 악의적인 의도로 메일 시스템에 접근하여 메시지 내용을 모두 볼 수 있다는 문제점을 안고 있다. 향후 정보통신이 발전함에 따라 이러한 피해는 더욱 늘어날 것이다. 이러한 문제점을 해결하기 위해서 메시지를 암·복호화하여 송·수신한다.

본 논문에서 제안한 메일 암호시스템은 메일을 송·수신할 경우 메일 내용을 ARIA 암호 알고리즘으로 암·복호화하여 송·수신자 외에는 그 내용을 알 수 없도록 한다. 제안한 메일 암호시스템은 공공기관 뿐만 아니라 민간기업, 그리고 일반인들에게도 유용하게 사용될 것이다.

참고문헌

[1] http://news.mt.co.kr/mtview.php?no=2001062512111611003&type=1

[2] http://www.softmail.co.kr/437

[3] http://blog.daum.net/sungji-ses/5627980M

[4] 히로시유키. “알기 쉬운 정보보호개론”, 인피니티 북스, 2008.

[5] 손승원, 이재광, 임종인, 전태일. “암호학과 네트워크보안”, McGraw-Hill Korea, 2008.

[6] http://www.md5decrypter.com/

[7] 임웅택. “안정성과 효율성을 갖춘 128-비트 블록 암호 알고리즘 설계 및 분석”, 박사학위논문, 2005.

[8] http://bloggernews.dkbnews.com/217