전방향 안전성이 보장되는 메일 프로토콜 설계

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

Design of the Mail Protocol with Perfect Forward Security

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

요 약 기존 메일 시스템은 송·수신자 이외에 제3자에 의해 공격당했을 경우 메일 내용이 그대로 노출된다. 이러한 문제점을 해결하기 위해 세션 키를 이용하여 안전하게 메일을 송·수신할 수 있는 메일 암호시스템을 설계한다. 메일 수신자는 세션 키를 통해 메일 내용을 복호화 하여 메시지를 확인한다. 기존 메일 시스템은 서버 관리자가 메일 내용을 볼 수 있었지만, 제안한 프로토콜은 암·복호화를 적용하기 때문에 서버는 메일을 저장해주는 역할만 할 뿐, 메일 내용은 볼 수 없도록 ARIA 암호알고리즘으로 암·복호화하여 안전성을 강화하고, 계산이 빠른 XOR 연산을 사용하여 연산량을 줄였다.

• **주제어** : 디피헬맨, 피지피, 아리아, 완전전달보안, 메일보안

Abstract When the existing mail system is attacked by the third party, its content is exposed fully. To solve this problem, designed is the mail encryption system which can send and receive mail safely by the sessionkey. The mail receiver opens encrypted mail with the session key. In the traditional mail system, the server administrator can view mail content. However, in the proposed protocol, the server can only save mail as encryption/decryption is applied. Also, the ARIA encryption algorithm is used in encryption/decryption for better safety, and fast XOR operations are used to reduce the amount of operations.

• **Key Words** : Diffie-Hellman, PGP, ARIA, Perfect Forward Security

1. 서 론

정보통신의 발전으로 인해 인터넷 사용자들이 급격하게 증가하고 있고 인터넷을 통해 정보를 전송, 저장, 그리고 사용되어지는 정보의 양이 급격하게 증가하고 있는 상태이다. 이러한 정보들은 개인이 어떠한 서비스를 이용할 경우 개인 정보들이 개인의 PC에만 저장되는 것이 아니라 서비스를 제공해주는 주체의 데이터베이스나 웹 기반의 이메일 서비스와 같이 우리가 자주 사용하고 있는 시스템에도 저장되어지고 사용자의 요구에 따라 이러한 정보들은 빈번히 이동·전송된다[1].

이렇게 전송 또는 저장되는 정보들은 해킹 및 바이러스와 같은 침해로 사용자의 개인정보가 누출 및 악용되고 있으며 그로 인한 프라이버시 침해가 일어나고 있다. 또한 서버를 관리하는 사람이 악의적인 목적을 가지고 있다면 서버 관리자들에 의해 사용자의 정보에 대한 악용, 남용 및 누출은 심각한 사회문제로 이슈화되고 있다.

*교신저자 : 신승수(shinss@tu.ac.kr)
접수일 2011년 6월 1일 수정일 2011년 6월 20일 게재확정일 2011년 6월 25일

최근 보고서에 의하면 악의적인 내부 공격자에 의한 개인정보 침해사건은 전체 사건의 59%를 차지하고 있는 것으로 보고되었으며, 그 위험성은 전 세계적으로 아주 심각한 상황이다. 또한 국내에서도 옥션 해킹사고, 하나로 텔레콤의 개인정보유출등과 관련된 사고로 인해 방송, 금융, 통신, 의료 사회 전반에 개인정보유출방지에 대한 논의가 진행 중이다[2].[3].

인터넷 범죄가 늘어나고 있고 그 위험성은 날로 증가하고 있으며 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[4]. 그러나 PGP는 이메일의 기밀성과 인증을 제공하지만 전방향 안전성을 보장하지 않는다. 일반적으로 키 교환 프로토콜에서는 전방향 안정성을 보장하기 위해서 Diffie- Hellman 키 교환을 사용한다. 그러나 이메일과 같은 store-and-forward 시스템에서는 수신자가 송신자와 지속적으로 통신을 유지할 수 없기 때문에 이 방식은 Diffie-Hellman 키 교환 기법을 적용하기 어렵다[5],[7]. 이메일 프로토콜에서 요구되는 안전성은 인증과 메시지 기밀성과 전방향 안정성이다. 전방향 안전성이란 사용자와 서버들의 룽텀 비밀키가 노출되더라도 그 이전에 전송된 암호화된 이메일 메시지에 대한 정보를 얻을 수 없어야 함을 의미한다.

본 논문의 구성은 다음과 같다. 2장에서는 메일 시스템에 대해서 분석하고, 3장에서는 메일 프로토콜을 설계한다. 그리고 4장에서는 비교 및 분석하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

보안 메일에도 여러 가지 종류가 있고, 그 방법과 성능이 다르므로 구체적으로 따져봐야 한다. 기존 웹 메일 시스템의 취약점 분석과 메일 암호시스템이 갖춰야할 기본 요건과 기술적인 특성에 대하여 분석한다[6].

2.1 웹 메일 시스템의 취약점 분석

기존 메일 시스템은 송신자가 메일을 전송할 경우 수신자가 아닌 메일 서버관리자 혹은 악의적인 목적을 가진 제3자에 의해 그들이 원하는 메일을 언제든지 열어볼 수 있다. 메일은 송·수신자만이 그 내용을 볼 수 있어야 하는데, 이는 기존 메일 시스템이 메일의 내용을 그대로 노출하고 있다는 취약점을 내포하고 있다. 기존 메일 시스템은 외부의 불특정 침입자로부터 쉽게 ID/PW를 해킹당하고 유출된 ID/PW를 이용하여 마치 자신인 것처럼 정식으로 로그인하여 메일을 열람할 수 있다. 또한 메일 시스템을 해킹하여 메일을 통째로 퍼가는 경우도 있다. 이렇게 외부인이 침입하는 것에 대한 대책은 패치를 하거나 백신을 설치, 방화벽, 침입 탐지기를 설치하여 정규 사용자 이외에는 들어오지 못하게 막는 것이 있는데 현재로선 ID/PW를 해킹당하지 않도록 하는 방법뿐이다.

2.2 메일 암호시스템이 갖춰야할 기본 요건과 기술적인 특성

보안 메일에도 여러 가지 종류가 있고, 그 방법과 성능이 다르므로 구체적으로 따져봐야 한다. 실제로 보안메일은 예전에도 여러 가지 형태로 보급이 시도되었으나 성공적이지 못하였다. 그 이유는 범용 솔루션으로서의 보편타당성 측면에서 가치를 형성하는데 실패했기 때문이다. 이를 보완하기 위해 메일 암호 시스템이 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 대신, 스스로 수신인의 계정을 만들어서 거기에 전달해 놓고 수신인에게 어디로 와서 편지를 확인하라는 일반적인 안내 메일을 대신 발송하는 방식이 사용되고 있다.

○ 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 전달 받을 수 없었다. 최근의 보안메일은 이 방법 대신 개인키를 안내 메일에 첨부파일로 보냄으로서 이 문제를 해결하고 있다.

○ 보안성과 편의성

공개키 기반의 가장 확실한 인증 방법은 사용자 인증 방식이지만, 1:1 사용을 전제로 하였기에 사용이 제한적

이고 까다롭다. 그러므로 사용 목적에 따라서 엄격한 보안을 요구하는 경우는 원칙을 철저히 준수하되, 약간의 융통성을 둬서 편의성을 더욱 강조할 수 있어야 한다.

○ 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 문서 보안관리 내용들이 함께 하여야 한다.

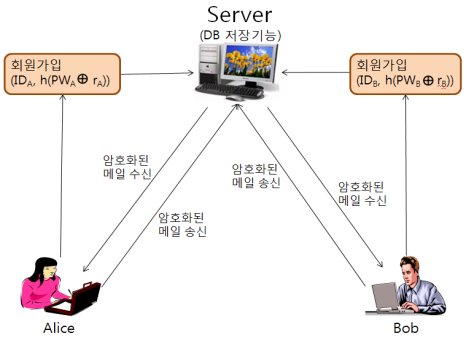
일반적인 메일이나 그룹웨어 등은 사용자가 자신의 계정으로 로그인하여 메일 내용을 암호화하지 않고 평문 상태로 서버에 전달하게 된다. 국내 유명포털인 네이버나 다음의 경우 암호화 기법인 MD5나 SHA-1을 사용하여 ID나 PW를 암호화하여 처리하고 있으나 이들도 메일 내용에 대한 보안은 전혀 이루어지지 않고 있다. 대부분의 국내 웹 메일 서버들은 메일 내용을 암호화하는 것에 대한 고려가 없는 경우가 많다. 최근 시장동향을 보면 보안 문제가 큰 이슈로 부각되고 있으며 웹사이트 해킹이나 내부 정보 해킹은 크나큰 문제가 되고 있다. 이는 메일 서버 관리자가 사용자들의 ID/PW 등의 개인정보를 알고 있고, 메일 내용 또한 알아낼 수 있기 때문이다. 개인 정보 유출 사고는 빈번히 일어나고 있다. 이처럼 다음, 네이버 등 국내 대부분 포털사이트의 웹 메일이 웜·바이러스 유포, 개인정보 유출, 나아가 컴퓨터를 마비시킬 수도 있는 심각한 취약점들이 있다.

본 논문에서는 기존 메일 시스템의 메일 관리자가 악의적인 목적으로 메일의 내용을 열람하거나 혹은 제3자의 악의적인 공격으로 인해 메일의 내용을 열람을 했을 경우 모든 내용이 그대로 노출되는 문제점을 해결하기 위해 메일 내용을 송·수신 하는 쌍방 간의 합의된 비밀키로 암·복호화하여 악의적인 의도로 메일에 접근했을 경우에도 비밀 키가 노출되지 않는 한 메일 내용을 알 수 없도록 프로토콜을 설계하고자한다.

3. 제안 프로토콜

3.1 메일 암호시스템 구성도

본 논문에서는 메일 암호시스템이 제3자의 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. 제안한 메일 암호시스템의 구성도은 그림 1와 같다.



[Fig. 1] Configuration of Mail System

3.2 제안 프로토콜

메일 암호시스템은 등록 단계, 로그인 단계, 세션 키 교환 단계, 메일 송신, 메일 수신, 받은 편지함·보낸 편지함의 순서이다. 본 논문에서 사용할 기호는 표 1과 같다.

[Table 1] Parameters

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

3.2.1 등록 단계

Alice는 서비스를 받기위해 서버에 회원가입을 하는 등록 절차는 다음과 같다.

① 먼저, Alice는 난수 r_A를 선택하여 $h(PW_A \oplus r_A)$를 계산한 값과 ID를 서버에게 보낸다.

② 서버는 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 데이터 베이스에 저장한다.

③ 서버는 Alice에게 H_{SA}를 보낸다.

④ Alice는 서버로터 받은 정보 H_{SA}를 저장한다.

3.2.2 로그인 단계

Alice가 서버에 로그인하기 위해서 ID와 PW를 입력하면 서버는 DB에 저장된 데이터와 Alice로부터 받은 정보인 $ID_A, h(PW_A \oplus r_A)$ 값을 비교하여 같을 경우 로그인이 승인이 되고, 같지 않을 경우 로그인이 승인되지 않는다. 로그인 단계는 다음과 같다.

① Alice가 $ID_A, h(PW_A \oplus r_A)$을 입력하고 서버로 부터 받은 정보 $H_{SA} \oplus h(PW_A \oplus r_A)$와 난수 N_A을 서버에게 전송한다. 즉, $ID_A, N_A, h(H_A \oplus N_A)$을 전송한다.

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

3.2.3 세션 키 교환 과정

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

① Alice는 $h(PW_A \oplus r_A), N_A$와 Bob의 ID_B을 이용하여 $h(H_A \oplus N_A \oplus ID_B)$을 계산하고, 메시지 M_1을 서버에게 전송한다. 즉,
$M_1 = \{N_A, ID_A, ID_B, h(H_A \oplus N_A \oplus ID_B)\}$이다.

② 서버는 DB에 저장된 Alice의 정보를 이용하여 $H_{SA} \oplus h(ID_A \oplus x_S), h'(PW_A \oplus r_A)$을 계산한다. M_1 속에 들어있는 정보 N_A, ID_B을 이용하여 $h(H_A \oplus N_A \oplus ID_B)$와 같은지를 비교하여 Alice를 인증한다.

③ 서버는 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_2을 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 서버로부터 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 해시함수가 같은지를 검증한다. Alice는 Bob과 메시지를 암·복호화 하기 위한 정보를 M_3정보에 포함시켜 M_1, M_3을 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_B을 이용하여 세션 키를 추출해 내고 $h(K)$와 같은지를 검증한다.

3.2.4 메일 송신

메일을 송신하는 절차는 다음과 같다.

① Alice는 메일을 작성한다.

② ARIA 암호 알고리즘을 이용해 메시지를 세션 키로 암호화한다. 즉, $E_{K_{AB}}(M)$이다.

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

3.2.5 메일 수신

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

① Alice로부터 전송된 수신 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 확인 했던 메일을 다시 확인하기 위해서는 $h(PW_B \oplus E_A)$ 값을 다시 입력한다.

④ 입력한 $h(PW_B \oplus E_A)$값이 일치하면 메일의 재확인이 가능하고, 일치하지 않으면 메일의 재확인이 불가능하다.

4. 분석

본 논문에서 제안하는 메일 프로토콜은 연산양이 적어 계산이 빠르고 송·수신자끼리 세션 키를 교환하여 메일 내용을 암호화하기 때문에 송·수신자 외에는 메일의 내용을 알 수 없으므로 안전하게 메일을 송수신 할 수 있다. 제안한 프로토콜을 단계별로 비교 및 분석을 한다.

4.1 단계별 분석

(1) 등록 단계 : 공개키 기반의 웹 메일 시스템에서의 메일 서버 관리자는 사용자의 ID/PW를 알고 있기 때문에 개인 정보 유출 사고도 빈번히 일어나고 메일의 내용을 그대로 볼 수 있었다. 제안한 메일 암호 시스템에서는 사용자 Alice의 ID/PW, 사용자 Alice가 선택한 난수를 가지고 해시 함수를 통해 메일 서버관리자나 악의적인 목적을 가진 제3자가 사용자의 신상 정보를 알 수 없도록 한다.

(2) 로그인 단계 : 공개키 기반의 웹 메일 시스템에서 사용자 인증을 할 때는 메일 서버 관리자가 사용자의 모든 개인 정보를 알고 있어야 인증이 가능했다. 제안한 메일 암호 시스템에서는 사용자가 회원가입 시, 신상 정보들을 해시함수로 해시 연산한 값을 가지고 사용자 인증을 하기 때문에 메일 서버 관리자가 사용자의 Password를 알고 있지 않아도 사용자 인증이 가능하다.

(3) 송신 단계 : 공개키 기반의 웹 메일 시스템의 메일 서버 관리자들은 임의로 메일 내용을 열람 할 수 있기 때문에 메시지 기밀성이 보장되지 않는다. 제안한 메일 암호 시스템에서는 이러한 메시지 기밀성이 보장된다. 메시지 기밀성은 전송되는 메일 내용에 대한 정보를 정당한 수신자 이외에 얻을 수 없어야 하는 것을 말한다. 송신 단계에서는 송·수신자가 세션 키 교환과정을 거치지만 사용자의 정보들이 모두 해시 연산을 통한 값이므로 메일 서버 관리자는 세션 키를 알 수 없다.

(4) 수신 단계 : 공개키 기반의 웹 메일 시스템의 메일 서버 관리자들은 메일을 송·수신하는 과정에서 메일의 내용을 그대로 볼 수 있었다. 제안한 메일 암호시스템에서는 메일을 송·수신하는 사용자들끼리 메일을 암·복호화 할 때 사용하는 세션 키를 교환하기 때문에 메일 서버 관리자는 세션 키를 가지고 있지 않아 메일의 내용을 복호화 할 수 없다. 즉, 메일 서버 관리자라고 하더라도 메일을 저장하여 송·수신만 할 뿐 메일의 내용은 알 수 없다. 또한, 사용자 Bob가 세션 키를 통해 사용자 Alice가 보낸 메일이 맞는지 아닌지 상대방 인증도 가능하다.

4.2 안전성과 효율성 분석

본 논문에서 제안한 프로토콜에 대한 추측공격, 재전송공격, 전방향 안전성, 서버 비밀키 추측공격, 위장공격에 대한 안전성을 분석하고 표 2에서는 이러한 문제에 대해 공개키 기반의 프로토콜[5]와 제안한 프로토콜을 비교하였다.

(1) 추측공격 : 제안한 프로토콜에서는 ID와 PW에 관한 정보를 모두 해시함수로 계산되어 서버에 저장하기 때문에 ID와 PW에 관한 정보를 추측할 수 없다. 또한, 해시함수의 일방향성과 난수의 예측불가능성 때문에 어떤 경우에도 ID나 PW를 추측하기 어렵다.

(2) 재전송 공격 : 제안한 프로토콜에서는 공격자가 세션 키를 알기 위해서는 $h(HA \oplus NA \oplus IDA \oplus IDB)$를 알아야 한다. 그러나 사용자는 매 세션마다 다른 난수를 사용하기 때문에 $h(HA \oplus NA \oplus IDA \oplus IDB)$와 관련된 정보를 알 수 없다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

(3) 전방향 안전성 : 공격자가 사용자의 개인키나 패스워드를 알아냈다 하더라도 이전의 사용자가 사용했던 어떠한 세션 키도 알 수 없을 경우, 프로토콜이 전방향 안전성을 만족한다고 한다. 제안한 프로토콜에서는 세션 키 교환단계에서 ID, PW를 해시함수를 이용한 해시 값을 연산한 값을 사용하기 때문에 이전에 사용했던 어떠한 세션 키도 알 수 없으며 공격자가 사용자의 ID를 안다고 해도 공격자는 서버의 비밀 키와 사용자 Alice가 선택한 난수를 모르기 때문에 어떠한 세션 키도 알 수 없다.

(4) 서버 비밀키 추측공격 : 서버의 비밀 키를 사용하여 암호화된 메시지는 많이 사용되는데, 공격자가 서버의 비밀 키를 사용하여 메시지를 가로챌 수는 있다. 하지만 가로챈 메시지로부터 서버의 비밀 키에 관한 정보를 유추하는 것도 해시함수의 일방향성과 난수의 예측불가능성 때문에 어렵다. 따라서 정당한 사용자라도 해시함수와 난수의 성질 때문에 서버의 비밀 키를 알 수 없다.

(5) 위장 공격 : 공격자는 H_A, N_A를 만들 수는 있다. 하지만 정당한 사용자 Alice 또는 Bob가 선택한 $H_A=h(PW_A \oplus r_A)$, N_A를 알아낼 수 없기 때문에 세션 키를 알 수 없다. 그러므로 제안한 프로토콜은 위장공격에 안전하다.

[Table 2] Comparison of protocol safety

	추측 공격	재전송 공격	전방향 안전성	서버 비밀키 추측공격	위장 공격
공개키 기반의 프로토콜	×	○	○	×	○
제안한 프로토콜	○	○	○	○	○

다음은 제안한 프로토콜에 대한 효율성에 대하여 분석한다. 표 3에서 보면, 공개키 기반의 프로토콜[5]와 제안한 프로토콜의 계산 비용은 비슷한 것을 알 수 있다. 먼저 랜덤 정수 생성횟수는 공개키 기반의 프로토콜이 제안한 프로토콜보다 1회 많고, 연산 회수는 공개키 기반의 프로토콜과 제안한 프로토콜이 동일한 회수를 나타내고 있다.

그러나 공개키 기반의 프로토콜은 지수연산이고 제안한 프로토콜은 XOR연산을 사용하기 때문에 연산 속도 측면에서는 제안한 프로토콜이 월등하다고 할 수 있다. 공개키 기반의 프로토콜과 제안한 프로토콜의 해시 연산 회수는 약간 차이가 나지만, 비교 연산은 공개키 기반의 프로토콜이 지수연산이고 제안한 프로토콜은 XOR연산이기 때문에 비교 연산회수가 많다 하더라도 제안한 프로토콜이 공개키 기반의 프로토콜보다 속도가 빠르다. 또한, 제안한 프로토콜은 공개키 기반의 프로토콜에 비해 통신비용이 감소하고 전체적인 효율성을 비교해보면 공개키 기반의 프로토콜에 비해 효율적이다.

제안한 프로토콜은 암·복호화를 적용하기 때문에 서버는 메일을 저장해주는 역할만 할 뿐, 메일 내용은 볼 수 없도록 ARIA 암호알고리즘으로 암·복호화하여 안전성을 강화하고, 계산이 빠른 XOR 연산을 사용하여 연산량을 줄였다. 기존 메일 시스템보다 편리성과 접근성은 조금 떨어지지만 무엇보다 안전하다는 장점을 가진다.

5. 결론

메일은 인터넷을 통해 누릴 수 있는 가장 오래된 서비스 중 하나이며, 가장 보편적인 수단이다. 기존 메일 시스템은 메시지를 암호화하지 않고 보내기 때문에 송·수신자 외에 제3자가 악의적인 의도로 메일 시스템에 접근하여 메시지 내용을 모두 볼 수 있다는 문제점을 가지고 있다. 향후 정보통신이 발전함에 따라 이러한 피해는 더욱 늘어날 것이다.

이러한 문제점을 해결하기 위해서 송신하기 전에 메시지를 암・복호화하여 송·수신하는 프로토콜을 설계하였다. 본 논문에서 제안한 메일 암호시스템은 메일을 송·수신할 경우 메일내용을 ARIA 암호 알고리즘으로 암·복호화 하여 송·수신자 외에는 그 내용을 알 수 없도록 하였다. 본 논문에서 제안한 메일 암호시스템은 인트라넷 망에서 사용가능하며 공공기관 뿐만 아니라 민간기업, 그리고 일반인들에게도 유용하게 사용될 것이다.

[Table 3] Comparison of protocol efficiency

		계산비용				통신비용	
		랜덤정수 생성회수	연산회수	해시 연산회수	비교연산	전체 전송데이터	서버 세션연결 후 전송 데이터
공개키 기반의 프로토콜[5]	사용자 A	1	7	1	1	13	7
	사용자 B	0	5	0	0		
	서버 S	1	8	1	1		
제안한 프로토콜	사용자 A	1	7	3	0	8	5
	사용자 B	0	4	1	1		
	서버 S	0	9	2	2		

REFERENCES

[1] Hyun Sook Rhee, Jong Hwan Park, Dong Hoon Rhee, “Public Key Encryption with Keyword Search in Multi-Receiver Setting”, Journal of the Korea Institute of Information Security and Cryptology, Vol. 19, No. 2, pp. 31-37, 2009.

[2] A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "2004 CSI/FBI Computer Crime and Security Survey", Ninth annual report of computer security society, CSI, 2004. For general information, refer to "http://goocsi.com or http://www.nipc.gov".

[3] Jin Wook Byun, “A Design of Efficient Keyword Search Protocol Over Encrypted Document”, Journal of IEEK, Vol. 46, No. 1, pp. 46-55, 2009.

[4] A. Bacard, The Computer Privacy Handbook: A Practical Guide to E-Mail Encryption, Data Protection, and PGP Privacy Software, Peachpit Press, 1995.

[5] Jeong Ok Kwon, Young Ju Koo, Ik Rae Jeong, Dong Hoon Lee, “An E-Mail Protocol Providing Secrecy without Using Certificated Public Keys”, Journal of the Korea Institute of Information Security and Cryptology, Vol. 19, No. 1, 2009.

[6] Seong Jae Lee, “The reason must use the security mail”, http://blog. daum.net/ sungji-ses/ 5627980M, 2007.

[7] Hee Hung Kim, Bon Yeol Gu, Seung Soo Shin, Kun Hee Han, “A Study on Mail Cryptography System using the ARIA”, proceedings of the KAIS Spring Conference, pp. 77-80, 2010.

저자소개

신 승 수(Seung-Soo Shin) [정회원]

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

<관심분야> : 암호프로토콜, 네트워크 보안, USN, 스마트 카드

한 군 희(Kun-Hee Han) [종신회원]

- 2000년 8월 : 충북대학교 컴퓨터 공학과 (공학박사)
- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야> : 콘텐츠 보호, 정보화 분석, USN