Signcryption 기반의 완전한 전방향 안전성을 제공하는 이메일 프로토콜

이창용*, 김대영*, 김상진**, 오희국*

*한양대학교, 컴퓨터공학과, **한국기술교육대학교 인터넷미디어공학부

A Signcryption based E-mail Protocol providing Perfect Forward Secrecy

Changyong Lee*, Daeyoung Kim*, Sangjin Kim**, Heekuck Oh*

*Department of Computer Science and Engineering, Hanyang University
**School of Internet Media Engineering, Korea University of Technology and Education

요 약

현재 PGP(Pretty Good Privacy)와 S/MIME(Secure/Multipurpose Internet Mail Extension)와 같은 여러 가지 이메일 보안 프로토콜들이 제안되어 사용되고 있으나 이들 프로토콜은 최근 중요시되고 있는 보안 요구사항인 전방향 안전성을 보장하지 못한다. 최근에 이 요구사항을 충족하는 이메일 보안 프로토콜들이 제안되었으나 현실적이지 못한 가정 하에 설계되었거나 효율성 측면에서 개선이 필요한 프로토콜들이다. 또한 일부 프로토콜들은 실제 완전한 전방향 안전성을 제공하지 못하고 있다. 이 논문에서는 이 부분을 개선하고, 완전한 전방향 안전성을 제공하는 안전한 이메일 프로토콜을 제안한다. 제안되는 프로토콜은 Zheng 의 signcryption 기법을 사용하여 효율적이고 안전한 인증을 제공한다.

I. 서론

정보통신 분야의 성장과 함께 이메일은 개인 간의 기본적 통신 수단에서 기업 간, 또는 기업과 소비자 간에 중요한 마케팅 수단으로도 발전되었다. 또한 이메일이 정보 데이터베이스로의 활용이 가능해 지고 금융 결제, 전자 상거래에서 필수 요소로 사용됨에 따라 이메일 보안에 대한 요구가 증대되고 있다.

가장 기본적인 메일 프로토콜인 SMTP(Simple Mail Transfer Protocol)[1]는 송신자의 진위를 확인하는 인증 과정이 없고 단순 평문의 전달에 그치는 프로토콜로 중간에 그 내용을 얼마든지 읽을 수 있고 수정하여 재전송도 가능하므로 여러 부분에서 보안에는 취약하다고 할 수 있다

이를 보완하기 위해 대표적으로 PGP[2]와 S/MIME[3] 등의 보안 프로토콜들이 제안되었다. 이 프로토콜들은 공개키 기반의 세션키를 사용한다. 하지만 이러한 방식으로는 사용자의 개인키가 노출 될 경우 이전의 모든 메시지의 복호화가 가능해 전방향 안전성(forward secrecy)을 보장 하지 못한다. OpenPGP의 전방향 안전성 확장 명세[4]에서 전방향 안전성을 보장하는 프로토콜을 제안하고 있지만 이것은 공개키의 수명을 짧게 하여 자주 바꾸는 방법으로 시간과 비용 면에서 효율적이지 않다.

2005년에 Sun 등은 완전한 전방향 안전성을 보장하는 이메일 프로토콜을 제안했지만 문제점을 가지고 있다. 김범한 등이 이를 수정해 완전한 전방향 안전성을 제공하는 이메일 프로토콜을 제안했으나 송신자와 수신자의 서버가 동일하다고 가

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터(ITRC) 지원사업의 결과로 수행되었음.

* 이 연구에 참여한 연구자는 '2단계 BK21사업'의 지원을 받았음.

정해 현실적이지 않으며 임의의 두 값을 유지해야 만 하는 등 현실적인 문제점이 있었다[5,6].

김대영 등은 송수신자의 서버를 분리한 현실적인 프로토콜을 제안했으나 수신자의 개인키가 노출될 경우 이전 교환된 메시지를 알 수 있어 완전한 전방향 안전성을 보장하지 못했다[7].

본 논문에서는 그 문제를 보강하여 현실적이면서 완전한 전방향 안전성을 보장하는 안전한 이메일 프로토콜을 제안한다.

II. 연구배경

1. 수학적 배경

정의 1 (Discrete Logarithm Problem (DLP)). 그룹 G의 생성자 α와 원소 β가 주어졌을 때, $\alpha^x = \beta$를 만족하는 x를 계산하는 문제를 말한다.

정의 2 (Computational Diffie-Hellman Problem (CDHP)). 그룹 G의 생성자 α와 원소 α^x, α^y가 주어졌을 때, α^{xy}를 계산하는 문제를 말한다.

현재까지 DLP, CDHP를 다항시간 내에 계산하는 것은 계산적으로 어렵다고 알려져 있다. 본 논문에서 제안하는 프로토콜의 안전성은 위의 문제들을 다항시간 내에 계산하는 것이 어렵다는 가정에 기반하고 있다.

2. Signcryption

Zheng은 1997년 서명과 암호화를 한 단계에 수행하는 signcryption 기법을 제안하였다[10]. Zheng에 의해 제안된 signcryption은 논리적으로 한 번에 서명과 암호화를 수행하여 기존의 서명 후 암호화에서 요구되는 계산 비용보다 더 적은 비용을 가진다.

다음 그림 1은 Zheng이 제안한 signcryption의 기본적인 프로토콜이다.

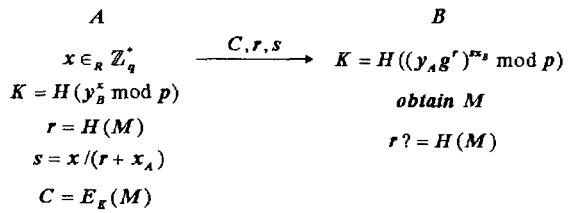

그림 1: signcryption 기본 프로토콜

A가 생성한 키 K에서 $y_B^r \bmod p$ 값은 B가 계산한 키 K에서 $(y_A g^r)^{sx_B} \bmod p$ 값과 결과적으로 일치하여 같은 키를 공유할 수 있게 되고, 이 과정에서 A는 자신의 개인키 x_A를 사용해 서명값을 계산하고 B는 A의 공개키 y_A를 사용하여 키값을 계산하므로 A를 인증할 수 있게 된다.

3. 이메일 프로토콜의 보안 요구사항

- 기밀성(confidentiality): 메시지의 내용을 오직 수신자만이 읽을 수 있어야 한다.
- 무결성(integrity): 메시지가 보내는 사람으로부터 떠나서 받는 사람에게로 이동할 때 메시지의 이동상에서 메시지가 위조 또는 변조되지 않은 것을 증명하는 것이 메시지의 무결성이다.
- 부인방지(non-Repudiation): 부인 방지란 메시지를 받은 사람이 메시지를 받지 않았다고 주장하는 것을 방지하도록 하는 메시지 수신 부인방지와 메시지를 보낸 사람이 자신이 메시지를 보내지 않았다고 주장하는 것을 방지하는 메시지 송신 부인 방지로 나누어진다. 메시지 수신 부인 방지는 ESMTP(Extended SMTP)[8]에서 지원하는 기능이므로 메시지 보안과는 어느 정도 거리가 있으므로 일반적으로 메시지 부인 방지라고 하면 송신 부인방지를 뜻한다.
- 사용자 인증(authentication): 실제로 메시지를 보낸 사람을 알 수 있어야 한다.
- 완전한 전방향 안전성(perfect forward secrecy): 모든 참여자의 장기간 키가 노출되어도 이전에 교환된 기밀성이 요구되는 메일의 내용이 노출되지 않아야 한다.
- 부분 전방향 안전성(partial forward secrecy): 일부 참여자들의 장기간 키가 노출되어도 이전에 교환된 기밀성이 요구되는 메일의 내용이 노출되지 않아야 한다.

III. 관련 연구

1. 표기법

이 논문에서 사용하는 표기법은 표 1과 같다.

표 1: 프로토콜 표기법

표기	의미
A	송신자
B	수신자
S	송신자의 SMTP 서버
P	수신자의 POP 서버
M	메시지
K_{UV}	U와 V간에 공유한 대칭키
g	위수가 소수 q인 군의 생성자
x_U	U의 개인키
$y_U = g^{x_U}$	U의 공개키
pwd_{UV}	U와 V간에 공유한 패스워드
N_U	U가 생성한 nonce
$H(M)$	메시지 M에 대한 해쉬값
$\{M\}_{K_{UV}}$	U, V간 대칭키 K를 이용한 메시지 M의 암호화
$E_{y_U}(M)$	U의 공개키 y_U를 이용한 메시지 M의 ElGamal 암호화
$MAC_K(M)$	메시지 M에 대한 키 K를 이용한 MAC 값
$M_1 \| M_2$	메시지 M_1과 메시지 M_2의 비트 결합

2. 전방향 안전성을 제공하는 안전한 이메일 프로토콜

2005년 제안된 전방향 안전성을 제공하는 안전한 이메일 프로토콜은 Diffie-Hellman 키 동의 기법[9]을 이용해 확립한 세션키를 사용해 메시지를 암호화하고 장기간 키가 노출되어도 세션키를 계산할 수 없도록 하여 전방향 안전성을 보장하였다. 그리고 송/수신자는 각자의 서버를 사용한다는 현실적인 가정을 바탕으로 제안되었다.

이 프로토콜의 경우 기본적인 이메일 보안 요구사항과 부분 전방향 안전성을 보장하지만 서버간의 전송과정에서 수신자의 메일 서버 P의 개인키가 노출될 경우 w_S를 알 수 있고 세션키 K_{AB}가 노출되어 완전한 전방향 안전성을 보장하지는 못했다. 만약 x_A, x_B, x_P 가 노출되고 공격자가 서버간 통신에서 $\{C \| r \| s\}_{K_{AB}}, E_{y_B}(g^{w_A}), E_{y_P}(w_s)$ 를 가로채 가지고 있다면 공격자는 $E_{y_P}(w_s)$에서 w_S를 알 수 있게 되고 $E_{y_B}(g^{w_A})$에서 g^{w_A}를 알 수 있게 된다. 공격자는 $g^{w_S w_A}$를 계산하여 K_{AB}를 얻을 수 있고 이것으로 $\{C \| r \| s\}_{K_{AB}}$를 복호화 하여 본문 메시지를 얻을 수 있게 된다. 결국 이 프로토콜은 상대적으로 많지 않은 연산으로 현실적 가정하에 부분 전방향 안전성을 보장하지만 완전한 전방향 안전성을 보장하지는 못한다.

IV. 제안하는 프로토콜

본 논문에서 제안하는 프로토콜은 이메일 보안 요구사항과 완전한 전방향 안전성을 보장하는 프로토콜로 2005년 제안한 프로토콜의 서버간 전송 부분에 개선을 하였다. Zheng이 제안한 signcryption 기법[10]을 이용하여 안전하면서 효율적인 인증을 수행하고, 이전 프로토콜에서는 w_S값을 수신자 서버의 공개키로 암호화하여 전송하는 것에 그쳤던 과정을 Diffie-Hellman 기법[9]을 사용한 세션키 성립 방식을 서버간 통신에도 적용하여 서버의 개인키가 노출되어도 이전 전송된 문서의 내용을 알 수 없게 하였다.

1. 프로토콜의 가정

- 송/수신자는 서로의 인증된 공개키를 가지고 있다.
- 송/수신자는 각자 자신의 메일 서버와 패스워드를 공유하고 있다.
- 완전한 전방향 안전성을 논할 때 장기간 키의 노출은 각 사용자/서버의 개인키뿐만 아니라 서버와 공유된 패스워드의 노출까지 의미한다.

2. 프로토콜

제안하는 프로토콜은 송신단계, 서버간 메시지 전송 단계, 수신 단계로 나뉜다.

(1) 송신 단계

- A는 첫 단계로 S에게 ID_A, N_A를 보낸다.
- S는 g^{w_S}의 해쉬값과 N_A를 비트연산 한다. 이를 다시 중간자 공격을 방어하기 위해 미리 공유한 pwd_{SA}를 이용하여 생성한 대칭키 K_{AS}로 암호화한 값 $\{H(g^{w_S}) \| N_A\}_{K_{AS}}$를 g^{w_S}와 함께 A에게 보낸다.
- A는 S로부터 온 메시지의 유효성을 확인하고 signcryption을 수행하게 된다. A는 임의의 정수 w_A와 x를 생성하고, x를 이용해 세션키 $K_1 \| K_2 = H(y_B^x)$를 생성한다. K_1, K_2는 $C = \{M\}_{K_1}$

과 $r = MAC_{K_2}(M)$을 계산하는데 사용되어 메시지를 암호화 하고 무결성 검증 부분에 활용된다. 마지막으로, 서명값 $s = x/(r + x_A)$을 계산한다.

- A는 $K_{AB} = g^{w_S w_A}$로 $C \| r \| s$를 암호화한 값과 B가 K_{AB}를 생성하기 위한 값 g^{w_A}를 B의 공개키로 암호화한 값을 S에게 보낸다. 이 때, g^{w_A}를 B의 공개키로 암호화했기 때문에 서버는 g^{w_A}를 확인할 수 없고, 결국 K_{AB}를 생성할 수 없어 메시지를 볼 수 없다. signcryption 기법은 전방향 안전성을 보장하지 않기 때문에 전방향 안전성을 보장하는 세션키로 r또는 s를 암호화 해야 한다.

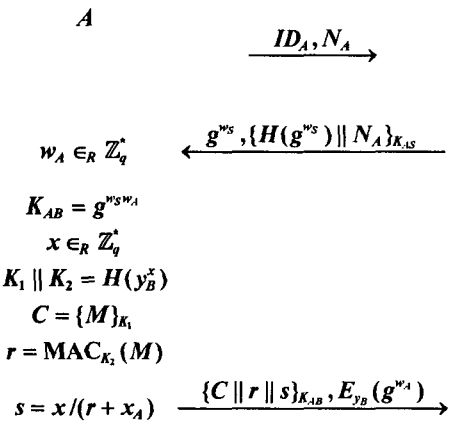

그림 2: 제안하는 프로토콜의 송신과정

(2) 서버 간 전송단계

- S는 이메일 전송을 위해 P에게 *request* 메시지를 보낸다.
- P는 임의의 정수 w_P를 생성하고 g^{w_P}를 생성하여 그 해쉬값 $H(g^{w_P})$를 자신의 개인키 x_P로 서명한다. 그리고 $g^{w_P}, H(g^{w_P})_{x_P}$와 함께 인증서 $Cert$를 S에게 보낸다.
- S는 받은 g^{w_P}의 무결성을 검증하고 자신이 생성한 임의의 정수 w_S를 이용하여 $K_{SP} = g^{w_S w_P}$를 생성한다. 이 키 K_{SP}를 사용하여 w_S를 암호화하고 $\{w_S\}_{K_{SP}}$를 A로부터 받은 값인 $\{C \| r \| s\}_{K_{AB}}, E_{y_B}(g^{w_A})$ 와 함께 P에게 전송한다.

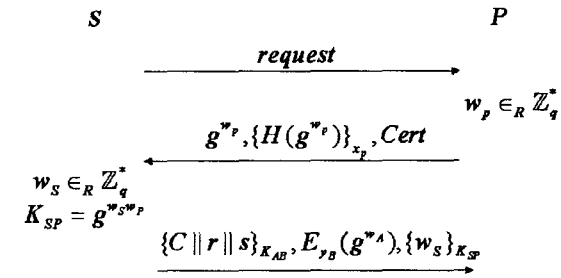

그림 3: 제안하는 프로토콜의 서버 간 전송단계

(3) 수신 단계

- B는 P에게 메일이 있는 지 요청하고, 만약 메일이 있다면 $ID_B, N_B, g^{w_B}, \{H(g^{w_B})\}_{K_{BP}}$를 보낸다. 여기서 K_{BP}는 pwd_B를 이용하여 생성한 대칭키이다.
- P는 B로부터 온 메시지의 유효성을 확인하고, 임의의 정수 값 w_P와 B로부터 온 값 g^{w_B}를 사용해 $K'_{BP} = g^{w_B w_P}$를 생성한다. 그리고 S로부터 온 메시지 중 $E_{y_P}(w_S)$를 복호화한 뒤 w_S를 구한다. 그리고 $H(g^{w_P})$, w_S, N_B를 K'_{BP}로 암호화해서 g^{w_P} 와 $\{C \| r \| s\}_{K_{AB}}, E_{y_B}(g^{w_A})$를 B에게 보낸다.
- B는 $K'_{BP} = g^{w_B w_P}$를 생성해 w_S, g^{w_A}를 복호화한다. 다시 구한 값으로 $K_{AB} = g^{w_A w_B}$를 생성하고 C, r, s를 복호화한다. 그리고 unsigncryption을

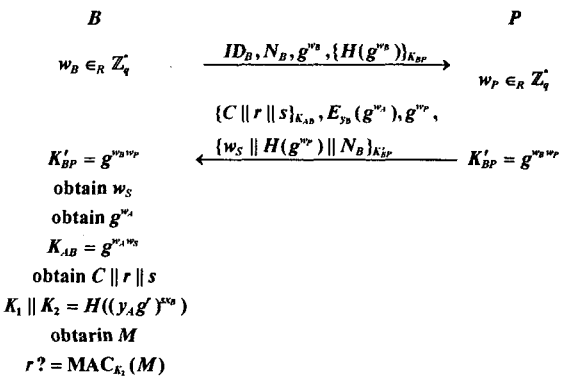

그림 4: 제안하는 프로토콜의 수신단계

수행하게 되는데 세션키 $K_1 \| K_2 = H((y_A g^r)^{sx_B})$를 생성하고 M를 얻어 $MAC_{K_2}(M)$값을 확인해 맞으면 수용한다.

V. 프로토콜 분석

- 기밀성: 메시지 M은 키 K_1으로 암호화 되어 기밀성을 보장한다.
- 인증: 수신자 B는 송신자 A의 공개키를 가지고 있고 A의 개인키 x_A로 서명을 했으므로 B는 A를 인증 할 수 있다.
- 무결성: $MAC_{K_2}(M)$값을 이용하여 무결성을 보장한다.
- 부인방지: 수신자 B는 송신자 A의 서명값 s를 확인할 수 있기 때문에 부인방지가 가능하다.
- 완전한 전방향 안전성: 제안하는 프로토콜을 완전한 전방향 안전성을 보장한다. 만약 공격자가 이전 메시지를 모두 도청해서 가지고 있고, A,B,S,P의 장기간 비밀키가 노출 되었다고 가정해도 이전 세션키를 얻기 위해서는 r 또는 s를 알아야 하는데 대칭키 K_{AB}로 암호화 되어 있고, 서버간 전송과정에서도 w_S값을 대칭키 K_{SP}로 암호화해서 전송하므로 이전 세션키를 알 수 없다. 그러므로 본 프로토콜은 완전한 전방향 안전성을 제공한다.

VI. 결론

본 논문에서는 완전한 전방향 안전성을 제공하는 안전한 이메일 프로토콜을 제안하였다. 제안하는 프로토콜은 이전 이메일 보안 프로토콜에 비해 연산량이 많이 증가하지 않았고, 송/수신자는 물론 송/수신 서버의 장기간 비밀키가 전부 노출되어도 이전 메시지의 내용을 알 수 없게 설계되어 완전한 전방향 안전성을 보장한다. 그리고 보내는 서버와 받는 서버가 동일해야 한다는 다소 비현실적 가정을 배제하고 송/수신 서버를 분리하여 현실적인 가정을 하였다는 장점이 있다.

참고문헌

[1] J. Postel, "Simple Mail Transfer Protocol," STD 10, RFC 821, 1982.

[2] J. Callas, L. Donnerhacke, H. Finney and R. Thayer, "OpenPGP Message Format," RFC 2440, 1998.

[3] B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," RFC 3851, 2004.

[4] I. Brown, "Forward Secrecy Extensions for OpenPGP," draft-brown-pgp-pfs-04, http://www.links.org/dnssec/draft-brown-pgp-04.html

[5] H. Sun, B. Hsieh and H. Hwang, "Secure E-mail Protocols Providing Perfect Forward Secrecy," IEEE Communication Letters, vol. 9, no. 1, pp. 58-60, 2005.

[6] 김범한, 구재형, 이동훈, "완전한 전방향 안전성을 보장하는 이메일 프로토콜," 한국정보보호학회 충청지부 학술대회, 2005.

[7] 김대영, 김상진, 오희국, "전방향 안전성을 제공하는 안전한 이메일 프로토콜," 한국정보보호학회 영남지부 학술발표회논문집, pp. 86-92, 2006.

[8] A. Dent, "Flaws in an E-Mail Protocol of Sun, Hsieh, and Hwang," IEEE Communication Letters, vol. 9, no. 8, pp. 718-719, 2005.

[9] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. 22, pp. 644-654, 1976.

[10] Y. Zheng, "Digital signcryption or how to achieve cost (signature and encryption) << cost (signature) + cost (encryption)," CRYPTO '97, LNCS 1294, pp. 165-179, 1997.