http://dx.doi.org/10.14400/JDC.2016.14.12.201

메일 프락시를 통한 사용자 상호인증 방법과 안전한 메일 플랫폼에 대한 연구

안효범*, 이수연**
공주대학교 공과대학 정보통신학부*, 백석문화대학교 컴퓨터공학부**

The Study on Secure Mail Platform and Mutual Authentication Using Mail Proxy

Hyo-Beom Ahn*, Su-Yeon Lee**
Division of Information and communication, Kongju National University*
Division of Computer Engineering, Baekseok Culture University**

요 약 메일 시스템은 기업 간 거래와 같은 중요한 내용을 전달하는 목적에 사용된다. 그러나 메일 시스템에서 메일 주소를 변경하여 보내는 공격은 어렵지 않다. 기업 간 거래에서 메일 서버를 인증하는 것과 메일 서버에 등록된 사용자를 인증하는 것은 매우 중요하다. 본 논문에서 제안하는 시스템은 기업 환경에서 송신자와 수신자의 인증과 권한을 확인하는 프락시를 두어 기업 간 거래 사기를 방지할 수 있는 메일 프락시를 제안하고자 한다. 제안된 안전한 메일 플랫폼은 프락시를 기반으로 메일서버들의 도메인을 구성하고, 도메인에 속한 메일 서버들을 확인하고 사용자를 상호인증(mutual authentication)하여, 메일 송신자와 수신자가 정당한 사용자일 경우 기밀성(confidentiality)을 위한 비밀키를 교환하고, 암호화하여 메일을 송신한다. 본 논문에서는 상호인증 프로토콜과 키 교환 방법을 제안하고 Casper 검증기법을 이용하여 안정성을 검증하였다. 향후 연구로는 메일의 안전성을 위한 도메인구성 전반적인 플랫폼에 대하여 연구를 할 것이다.

주제어 : 상호 인증, 메일 서버, 메일 프락시, 키 교환, 사용자 인증, 도메인 관리

Abstract The purpose of Email system is used to transmit important information between companies in today. But Email system has vulnerabilities such that changing email address of sender by attacker. So it is important to authenticate mail server and user using mail server. This paper proposed mail proxy located between mail servers that evaluate authority and authenticate sender and receiver. The proposed email platform has some functions to compose trusted domain and to authenticate mail servers in the domain. Also, if sender and recipient are valid users in mail system, each exchanges a key for confidentiality and the sender sends an e-mail encrypted with exchanged key to recipient. In this paper, we propose a key exchange scheme in proposed platform and verify this protocol using Casper which is the formal analysis tool. In the future research, we will study the overall platform of the domain configuration for the security of mail.

Key Words : Mutual Authentication, Mail Server, Mail Proxy, Key Exchange, User Authentication, Domain Management

* "이 논문은 2015년 공주대학교 학술연구지원사업의 연구지원에 의하여 연구되었음", This work was supported by the research grant of the Kongju National University in 2015"
Received 31 October 2016, Revised 30 November 2016
Accepted 20 December 2016, Published 28 December 2016
Corresponding Author: Hyo-Beom Ahn
(Kongu National University)
Email: hbahn@kongju.ac.kr

ISSN: 1738-1916

1. 서론

전자우편은 아직까지도 민간과 기업에서 메시지를 전달하기 위하여 사용된다. 전자우편을 사용하는 목적은 인터넷을 통해 메시지를 전달하는 것이었으나 최근 들어 전자우편의 응용으로 전자우편주소(E-mail address)를 사용하여 가입자를 인증하는 응용이 늘고 있어, 전자우편주소가 인증 요소로서 사용되고 있다. 예를 들면, FaceBook과 Google+ 등과 같은 SNS(Social Network Service)에서 전자우편을 통해 사용자를 인증하는 목적으로 사용한다. 그러나 전자우편주소를 사용하는 인증은 전자우편을 통해 전자우편주소의 소유자만을 확인할 뿐 정당한 권한을 가진 사용자인지 확인하지 않는 보안 취약점을 내포하고 있고, 도덕적 해이로 인한 보안사고가 발행하고 있다[15]. 이러한 취약점은 기업에서 중요한 전자우편을 사용자 권한에 대한 아무런 검증 없이 처리할 수 있다는 문제를 제기 될 수 있다. 또한, 사용자에 대한 권한의 인증과 송신자에 대한 검증이 이루어지지 않아 스팸(spam), 피싱(phishing)과 같은 악의적인 의도에 노출되게 된다.

기존의 전자우편보안은 스팸메일, 피싱(phishing)과 같은 악의적 의도를 막기 위한 도메인을 이용한 방법과 사용자인증을 통한 메시지의 무결성(integrity)와 부인봉쇄(non-repudiation)을 목적으로 하는 방법인 두 종류로 나누어 볼 수 있다. 전자는 도메인 네임 서버를 이용하여 정당한 도메인 이름을 소유한 메일 서버로부터 전달 된 것인지를 판단함으로써 스팸과 피싱을 막는데 사용된다[2,3,4]. 후자는 공개키를 기반으로 하여 메일주소 소유자를 인증하고 메시지 무결성을 위하여 해시함수(hash function)을 사용한다[5,6,7].

스팸메일이나 피싱을 방지하기 위한 SPF[2], DKIM[3] 그리고 Sender ID[9]과 같은 방법은 사용자에 대한 인증과 메시지에 대한 무결성 및 부인봉쇄 서비스를 제공하지 못한다. 이러한 메일 시스템은 개인에 대한 인증을 단순히 패스워드를 이용하는 기존 방법을 사용한다. S/MINE, PGP는 공개키를 기반으로 하여 인증, 무결성, 그리고 기밀성을 제공하지만 개인에 대한 인증서를 통해 수행되기 때문에 공인된 인증기관을 사용 않을 경우 악의를 가진 사용자가 임의적으로 키를 생성하고, 수신자를 속일 수 있다.

본 논문에서는 위에 설명된 두 가지 방법의 취약점을 해결할 수 있는, 메일 프락시(mail proxy)를 이용한 방법을 제안한다. 제안된 방법은 메일 서버에 대한 인증과 메일 서버에 포함되어 있는 사용자들에 대한 인증을 통합하여 관리할 수 있는 안전한 메일 플랫폼을 제공한다. 또한, 메일 프락시를 사용하여 기밀성과 무결성을 제공하는 인증 방법과 기밀성을 제공하는 키 분배 프로토콜을 설계하고 검증을 하였다.

제안하는 메일 프락시를 이용한 메일의 인증 방법은 [8]에서 제안된 방법을 사용하였고 도메인을 이용하여 메일 프락시를 통한 메일 서버의 관리 기법을 제안하였으며 제안된 프로토콜은 보안 프로토콜들의 정형화 방법[10]인 정형검증도구인 CASPER[13]을 이용한 검증을 수행하였다. 제안된 메일 프락시는 검증을 통해 메일 서버와 연계를 통해 사용자가 유효한지를 검증하고 메일을 전송하는데 사용되는 일회용 키를 생성하는 역할을 담당한다. 또한, 기존의 메일 프락시가 하는 메일에 대한 필터링과 관찰(inspection)의 기능을 수행한다.

논문의 구성은 다음과 같다. 2장에서는 기존 메일 서버에서의 보안 기법에 대하여 분석하고, 3장에서는 안전한 메일 플랫폼에 대하여 제안하고, 4장에서는 제안 된 프로토콜을 정형검증기법을 통해 안전성을 분석하고 결론을 맺는다.

2. 기존연구

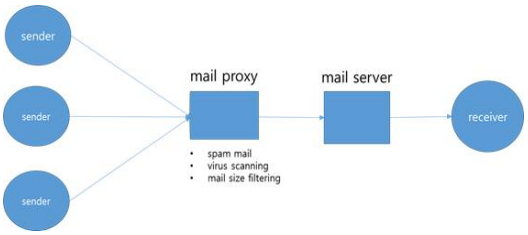
2.1 전자메일 보안

전자우편에서는 스팸 메일과 피싱을 방지하기 위한 메일 서버의 도메인에 대한 검증을 수행하기 위한 목적으로 사용되는 SPF(Sender Policy Framework), DKIM(Domain Keys Identified Message), 그리고 DMARC(Domain-based Message Authentication)이 사용된다[2,3,4]. 또한, 메시지의 무결성과 비밀성 그리고 부인 방지, 개인 인증 등의 서비스를 제공하기 위한 PGP(Pretty Good Privacy)[5], PEM(Privacy Enhanced Mail)[6], S/MIME(Secure Multi-Purpose Internet Mail Extension)[7]이 사용된다. 전자의 경우는 메일 시스템의 하부구조(infrastructure)를 기반으로 하여 송신 서버에 대하여 유효한지에 대한 검사를 수행하며, 메일 주소

를 통한 개인 인증은 제공하지 않는다. 후자의 경우에는 개인 인증서를 이용한 인증과 암호화를 하지만, 인증서를 개인이 생성할 수 있기 때문에 소속내의 정당한 사용자임을 증명하는 것은 어렵다.

2.2 메일 프락시(mail Proxy)

메일 프락시는 SMTP proxy 또는 메일 에이전트로도 불린다[1,6]. 일반적인 메일 프락시는 [Fig 1]에서와 같이 구성되며, 외부로부터 전달되는 메일의 내용이나 첨부파일을 검사한다. 메일 프락시는 메일 검사를 통해 바이러스 스캐닝(Virus Scanning), 파일유형 블록킹(File type blocking), 파일 크기 블록킹(file size blocking), 그리고 스팸 필터링(spam filtering)과 같은 기능을 수행한다. 그러나 메일 프락시는 송신자에 대한 인증을 수행하지 않는다. [Fig. 1]은 메일 프락시를 사용하는 기존의 메일 시스템 구성을 보여준다.



[Fig. 1] The role and organization of existing Mail Proxy

3. 안전한 메일 플랫폼

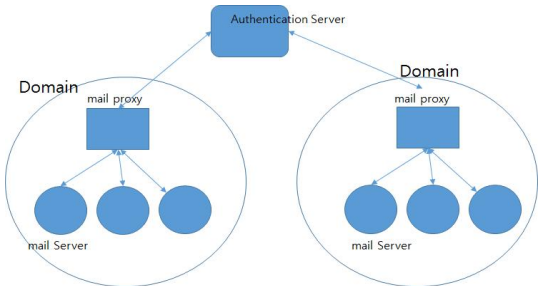
3.1 메일 플랫폼의 구성 및 기능

메일 플랫폼은 [Fig. 2]에서 보는 것 같이 메일 프락시들과 메일 서버로 구성이 된다. 하나의 메일 프락시는 여러 메일 서버를 멤버로 갖는 도메인을 관리한다. 제안하는 메일 플랫폼의 구성요소는 <Table 1>과 같다.

메일 프락시를 이용한 메일 플랫폼은 [Fig. 2]에서 보는 것과 같이 구성된다. AS(Authentication Server)는 메일프락시에 대하여 신뢰를 갖도록 인증기능을 수행한다. 인증 서버를 통해 메일 프락시들은 인증서를 발급받아 메일 서버와 신뢰관계를 형성할 때 사용된다.

<Table 1> Components of Mail platform

Components	description
Domain	Domain consist of mail servers as member by Proxy server
mail proxy	Mail proxy have function to manage members: 1) Add mail server in domain 2) remove mail server from domain
Mail Server	Mail server have roles which are authenticate valid user in mail system, sending and receiving mail to mail proxy in domain



[Fig. 2] Structure of Domain in mail platform

3.1.1 도메인 등록

메일 프락시는 메일 서버들의 도메인을 구성하고, 도메인을 통해 메일 서버들을 관리한다. 메일 프락시는 각 메일 서버에 대하여 자신의 도메인에서 사용될 ID를 발급하고, 도메인에 속한 메일 서버라는 것을 인증한다. ID를 생성하며 도메인에 가입하는 과정은 다음과 같은 단계를 갖는다.

단계1. 메일 서버(MS)는 메일 프락시(MP)에게 도메인에 가입하기 위한 정보를 보내다.

MS -> MP: CERT(MS), N1, ADDR_ms, DN_ms

여기서, CERT(MS)는 메일 서버의 인증서이고, N1은 Nonce이고 ADDR_ms는 메일 서버의 IP주소, 그리고 DN_ms는 DNS이름이다.

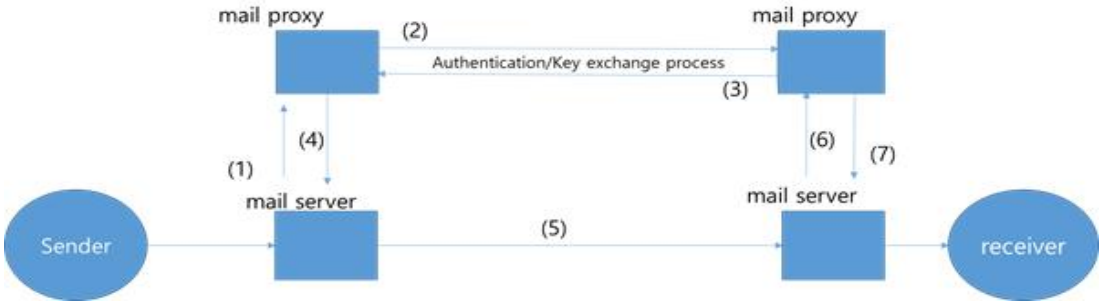
단계2. 메일 프락시는 메일 서버로부터 받은 인증서를 이용하여 도메인 ID를 보낸다.

MP->MS:

E(PUB(MS), D_id, N1, N2), CERT(MP)

여기서, E()는 암호화 알고리즘을 PUB(MS)는 메일 서버의 공개키를 의미한다.

단계3. 도메인ID를 받은 메일 서버는 도메인 ID와 인증서를 이용하여 메일 프락시를 검증하고, 도메인에서



[Fig. 3] The proposed mail platform to provide confidentiality and user authentication

사용할 멤버ID를 도메인ID를 사용하여 생성하여 보낸다.

MS: M_id <- CGA(D_id, PUB(MS))

MS->MP: E(PUB(MP), N2, M_id)

여기서, PUB(MP)는 메일 프락시의 공개키이고, CGA()는 CGA(Cryptographically Generated Address)를 구하는 함수를 의미한다.

단계4. 멤버ID를 받은 메일 프락시는 CGA로 전달 된 D_id를 제외한 나머지를 통해 메일 서버의 M_id가 유효한지를 검증하고 가입시킨다.

MP: (M_id, DN_ms, ADDR_ms) -> Database

위와 같은 단계로 진행되고 이때, M_id를 생성은 CGA(Cryptographic Generate Address) 방식[7]을 이용해서 생성한다. 이 M_id는 메일 프락시의 도메인과 MS에서 생성한 키를 이용하기 때문에 MP에서 메일 서버를 인증하는 요소로 사용할 수 있다.

3.1.2 도메인 탈퇴 및 제거

메일 프락시는 도메인에 가입된 메일 서버를 관찰하는 기능을 갖는다. 기존의 메일 프락시가 가지는 기능 중에 메일을 조사하여 스팸이나 피싱을 일으키는 메일이 있을 경우 메일 서버를 도메인에서 제거한다. 또한, 메일 서버가 도메인에서 탈퇴를 하고 다른 도메인에 가입할 수 있다. 이때에도 도메인 등록 과정을 거쳐 검증을 받는다. 메일 서버는 하나의 도메인에만 가입할 수 있고, 각 메일 프락시는 리스트를 서로 공유하여 이중 가입을 방지한다.

3.2 키 교환과 상호 인증을 위한 설계

제안하는 방법은 몇 가지 가정이 요구된다. 첫째, 사용자와 메일 서버와의 통신은 안전하고, 사용자의 등록은 안전한 절차에 의해서 신원확인 후 등록된다. 둘째, 메일 서버와 메일 프락시는 SSL(Secure Socket Layer)과 TLS(Transport Layer Secure)와 같은 네트워크 보안프로토콜이 사용된다. 셋째, 각 메일 서버와 연관된 메일 프락시(mail proxy)는 신뢰된 도메인(Trusted Domain)으로 구성되어 있다. 즉, 신뢰된 도메인은 별도의 신뢰된 기관을 가입과 탈퇴를 수행한다.

본 논문에서 제안된 방법은 메일 시스템에 인증과 키를 교환하기 위하여 메일 프락시(mail proxy)를 둔다. 메일 프락시는 첫째, 송신자와 수신자의 메일 서버에 대한 상호인증을 수행한다. 둘째, 메일을 암호화할 때 사용될 세션 키를 교환하는 작업을 수행한다.

제안된 메일 시스템은 [Fig. 3]과 같이 (1)-(7)로 구성되며 각 단계는 다음과 같은 절차를 수행한다.

- 단계1: 송신자가 수신자에게 메일을 보내면, 송신자 메일 서버(MS)는 메시지를 보내지 않고, 수신자의 정보를 자신의 메일 프락시(PS)에게 전달한다.

(1a) P-> msP: idP, idQ, Mail_Body

여기서 P: 송신자, idP: 송신자의 이메일주소, idQ: 수신자의 이메일주소, msP: P의 메일 서버, Mail_Body: 메일 내용

(1b) msP -> mpP: idP, idQ, Mail_Body

여기서 mpP: 송신자의 메일 프락시

- 단계2: 송신자의 메일 프락시(PS)는 수신자의 메일 프락시(PR)에게 자신의 인증서와 수신자에 대한 인증을 요구한다.

(2) mpP -> mpQ: mpP, idQ, ts, E(PR(mpP), H(mpP, idQ, ts)), CERT(mpP)

여기서 mpQ: 수신자, ts: 타임스탬프, CERT(X): X의 인증서, PR(X): X의 개인키(private key), H(M): M의 해시메시지(hash message)

- 단계3: 수신자의 메일 프락시(PR)는 회사에 등록된 수신자라면 송신자의 메일 프락시(PS)의 공개키를 이용하여 일회용 키 생성에 필요한 정보를 보낸다. 등록되지 않았다면 유효하지 않다는 메시지를 보낸다.

(3) mpQ -> mpP: mpQ, ts, n, E(PU(mpP), SK), E(PR(mpQ), H(mpQ||SK||ts)), CERT(mpQ)

여기서 PU(X): X의 공개키(public key), SK: mpQ가 임의로 생성한 세션 키(session key)

- 단계4 : 송신자의 메일 프락시(PS)는 수신자가 유효하다는 것을 확인하고, 일회용 키를 수신자의 메일 프락시(PR)가 보낸 정보를 이용하여 생성하고, 자신의 인증 정보와 송신자의 메일을 일회용 키로 암호화하여 메일 서버(MS)에게 전달한다.

(4) mpP -> msP: mpP, n, E(SK, idP||idQ||Mail_Body), HMAC(SK, mpP||n||idP||idQ||Mail_Body)

- 단계5: 암호화된 메일과 프락시(PS)의 인증정보는 메일 서버를 통해 수신자의 메일 서버(MR)로 전달된다.

(5) msP àmsQ: mpP, n, E(SK, idP||idQ||Mail_Body), HMAC(SK, mpP||n||idP||idQ||Mail_Body

- 단계6: 메일 서버(MR)는 메일 프락시(PR)에게 자신이 받은 메일을 전달하고, 메일 프락시는 송신자의 인증 정보를 검증한다.

(6) msQ -> mpQ: mpP, n, E(SK, idP||idQ||Mail_Body), HMAC(SK, mpP||n||idP||idQ||Mail_Body)

- 단계7: 암호화된 메시지를 복호화하여 수신자에게 전달한다. 검증이 실패한다면 전달된 메일을 삭제한다.

(7) mpQ àQ: idP, idQ, Mail_Body

송신자의 메일을 일회용 키로 암호화하기 위하여 키 생성 정보를 송신자에게 보내고 이를 확인하여 정당한 송신자인지를 확인할 수 있다. 또한 메일 프락시를 통해 회사에 등록된 사용임을 증명하기 때문에 송신자는 메일 주소의 유효성을 검증할 수 있다. 여기서 메일 프락시는 신뢰성 있는 인증기관으로부터 인증서를 발급 받아야 한다. 각 기업의 메일 프락시는 신뢰성 있는 기관에 메일 프락시를 등록하고 기관에서는 메일 프락시에 대한 정보를 제공하도록 하여야 한다. 제안된 방법은 최대한 기존의 메일 시스템을 유지하도록 하였고, 메일 클라이언트의 호환성을 유지하도록 설계하였다.

4. 제안된 프로토콜의 안전성 분석

보안프로토콜 중 인증방법은 개체를 식별하기 위하여 중요한 역할을 수행한다[16,17]. 이러한 보안 프로토콜을 검증하는 정형화 방법으로는 BAN-logic과 Casper/FDR이 많이 사용된다[11,14]. 본 논문에서는 본 장에서는 3장에서 제안한 메일 프락시를 사용한 키 교환과 상호 인증 프로토콜을 정형검증도구인 Casper를 이용하여 모델링하였다.

Casper 명세 중에 중요한 #Free variables, #Protocol Description, # 침입자 영역(#Intruder information)에 대한 표현이다[12]. 다른 명세 부분은 매우 간단하고 명확해서 자세한 설명은 생략하고자 한다.

#Free variables
P, Q : Agent
P_m, Q_m : Mail Server
P_p, Q_p: Proxy Server
skv: Secrete key
pkv: Public key
B: Mail body
SK: Session key
Td: TimeStamps
H: HashFunction
n: Nonce
InverseKey=(sky,pky), (SK,SK), (Td,Td), (n.n)

#Free variable 섹션 헤더에서는 #Protocol description

에서 사용되는 자유 변수의 타입 및 함수를 정의하고 있다. P와 Q는 송신자와 수신자의 식별자를 의미하고 Pm과 Qm은 송수신자의 메일 서버, Pp,와 Qp는 송수신자의 메일 프락시 서버의 식별자를 나타낸다. skv는 개인키 k를 의미한다. 그리고 SK는 두 Agent간의 세션 키를 의미한다. H는 해쉬 함수, Td는 타임스탬프, n은 임의의 난수를 의미한다.

#Protocol Description
0. → P : Q
1. P → P_m : P, Q, B
2. P_m → P_p : P, Q, B
3. P_p → Q_p : Td, skv, cert(P_p) H(Td, P_m ,Q)
4. Q_p → P_p : Td, n, SK, skv, cert(Q_p) H(Q_P, SK, Td)
5. P_p → P_m : n, skv, H(SK, n, P_p ,Td, P, Q, B)
6. P_m → Q_m : n, skv, H(SK, n, P_p ,Td, P, Q, B)
7. Q_m → Q_p : n, skv, H(SK, n, P_p, P, Q, B)
8. Q_p → Q : P, Q, B

#Protocol Description 영역은 제안된 프로토콜을 명세한 부분으로 P → P_m 는 사용자와 메일 서버간의 메시지 전송을 P_p → Q_m 는 프락시 서버와 메일 서버간의 메시지 전송을 나타낸다.

#Intruder information
Intruder = Mallory
IntruderKnowledge = {P, Q, P_m, Q_m, Mallory, v, u, SK}

#Intruder information 섹션 헤더에서는 통신 프로토콜을 공격하기 위한 공격자의 사전 정보를 표현한다. 예를 들어, 위의 명세 코드를 보면 공격자 호스트의 이름은 Mallory라고 설정하였으며 P, Q, P_m 그리고 Q_m은 송수신 메일 서버와 프락시 서버를 나타내고 있다.

본 논문에서는 공격자는 모든 호스트의 식별자를 도청을 통해 알 수 있다고 한다.

다음은 제안된 프로토콜을 보안 요구사항에 대해 암호학적 안전성을 분석한다.

#Specification
Secrete(P_P , H, [Q_P])
Secrete(P_P , SK, [Q_p])
Secrete(P_m , SK, [Q_m])
Secrete(Q_m , H, [Q_P])
Agreement(P ,Q, SK)

#Specification 부분은 제안된 프로토콜의 검증 속성을 표현한 부분이다. Casper script를 이용하여 명세화하기 위해 두 개체 간 사용된 정보에 대한 비밀성과 개체간 상호 인증을 만족해야한다. Secrete(P_P , H, [Q_P])의 표현은 "P_P는 H 정보틀 오직 Q_P만 알고 있다"라고 풀이할 수 있다. Secrete(P_P , SK, [Q_p])의 표현은 Q_P에서 생성된 세션 키(SK)에 대해 " P_P는 SK정보를 오직 P_P만 알고 있다"로 풀이할 수 있다.

▪ 기밀성(Confidentiality)
공격자가 메일 서버와 프락시의 ID 정보를 도청하여 소유하고 있다고 가정하자. 세션 키(SK)는 E(PU(mpP), SK) 즉, 메일 프락시의 공개키를 통해 생성하고 메일 프락시의 개인키를 통해 복호화되므로 공격자는 세션 키로 암호화 된 메시지를 복호화 할 수 없다. 따라서 메시지의 기밀성이 유지된다.

▪ 비연결성(stateless)
세션 키는 임의의 nonce를 통해 일회용 키로 만들어져서 매번 메시지를 인증 시 변경되기 때문에 각 인증 사이의 관계를 송수신자가 알 수 없다.

5. 결론

본 논문에서는 안전한 전자우편시스템을 구현하기 위하여 메일 프락시를 통해 송신자와 수신자를 인증하고, 키를 생성하여 메시지를 암호화하여 교환하도록 한 메일 플랫폼을 제안하였다. 이것은 기존의 메일 프락시가 했던 이메일 조사(mail message inspection)과 스팸 필터링(spam filtering) 뿐만 아니라, 메일 프락시를 통해 메일 서버로 부터 사용자의 인증을 수행한다. 그러나 제안된 방법은 메일 시스템을 변경해야하는 단점을 가지고 있지만, 수신자와 송신자를 확인하는 과정을 통해 스팸과 피

싱과 같은 공격을 방지할 수 있고, 메시지를 암호화함으로써 기밀성을 유지할 수 있다.

즉, 메일 서버는 사용자들에 대한 정보를 기업의 인사 시스템을 통해 전달받아 사용자 관리를 해야 하므로 사용자 등록 여부뿐만이 아니라 사용자 권한에 대해서 판단할 수 있다. 그러나 메일 프락시 간에 신뢰를 전제하지 않는다면 공격자는 메일 프락시를 가장하여 공격을 수행할 수 있기 때문에 메일 프락시들의 신뢰된 도메인을 구축해야한다. 따라서 메일 프락시간의 상호인증을 수행하며 세션키를 교환하여 송수신자의 상호 인증을 수행한다. 그리고 제안된 프로토콜은 Casper 검증도구를 사용하여 안전성을 분석하였다.

향후 연구로는 IoT환경 내에서 전자우편주소를 식별자로 사용할 수 있는 체계에서 정당한 사용자를 식별하기 위한 수단으로도 확장할 수 있고 자동화 검증도구인 AVISPA를 사용하여 좀 더 정밀한 분석을 하고자 한다.

ACKNOWLEDGMENTS

This work was supported by the research grant of the Kongju National University in 2015″

REFERENCES

[1] SMTP Proxy, https://en.wikipedia.org/wiki/SMTP_proxy

[2] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <http://www.rfc-editor.org/info/rfc7208>.

[3] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <http://www.rfc-editor.org/info/rfc6376>.

[4] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance(DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015,<http://www.rfc-editor.org/info/rfc7489>.

[5] J. Callas, L. Donnerhacke and D. Shaw, "OpenPGP Message Format", RFC4880, November 2007, <http://www.rfc-editor.org/info/rfc4880>.

[6] I. Brown and C. R. Snow, "A proxy approach to e-mail security," Software - Practice and Experience, Vol. 29, No. 12, pp. 1049-1060, October 1999

[7] T. Aura, RFC 3872, Cryptographically Generated Address(CGA), http://tools.ietf.org/html/rfc3972

[8] H.B. Ahn, J.H. Kim and J.H. Lee, "Study on Secure Mail System and User Authentication Using mail Proxy," MOBISEC2016 Symposium, 2016

[9] J. Lyon, M. Wong, Sender ID: Authenticating E-mail, RFC 4406, April, 2006. https://tools.ietf.org/html/rfc4406

[10] C. Cremers, S. Mauw, and E. de Vink, "Formal methods for security protocols: Three examples of the black-box approach," NVTI newsletter, Vol. 7, pp. 21 - 32, 2003.

[11] S. Yang, X. Li, A limitation of BAN logic analysis on a manin-the-middle attack, Journal of Information and Computing, Science ,Vol. 1, No. 3, (2006) 131 - 138.

[12] Formal System Ltd, FDR2 User Manual, Aug, 1999.

[13] Lowq, G., "Casper: A Compiler for the analysis of Security Protocols," In Proc. of the 1997 IEEE Computer Security Foundation Workshop X, IEEE Computer Society, Silver Spring, MD, pp, 18-30, 1997.

[14] Wessels, J., and CMG FINANCE BV. "Applications of BAN logic." Available from: http://www. win. tue. nl/ipa/activities/springdays2001/banwessels, 2001.

[15] Myung-Seong Yim, Moral Disengagement in Information Security Context: A Study of Antecedents and Outcomes, Vol. 11, No. 11, pp. 1-13, 2013.

[16] Tae-Hoon Yoo, Sang-Hun Lee, "Generation Method of Depth Map based on Vanishing Line using Gabor Filter", Journal of the Korea Convergence Society, Vol. 3, No. 1, pp. 13-17, 2012.

[17] Kwang-Jae Lee, Keun-Ho Lee, "Authentication Scheme using Biometrics in Intelligent Vehicle Network", Journal of the Korea Convergence Society, Vol. 4, No. 3, pp. 15-20, 2013.

안 효 범(Ahn, Hyo Beom)

- 1992년 2월 : 단국대학교 전자계산학과(이학사)
- 1994년 2월 : 단국대학교 전산통계학과 대학원 석사(이학석사)
- 2002년 8월 : 단국대학교 전산통계학과 대학원 박사(이학박사)
- 1997년 9월 ~ 2005년 3월 : 천안공업대학 정보통신과 부교수
- 2005년 3월 ~ 현재 : 공주대학교 정보통신공학부 교수
- 관심분야 : 네트워크 보안, 산업제어 보안
- E-Mail : hbahnr@kongju.ac.kr

이 수 연(Lee, Su Youn)

- 1990년 2월 : 단국대학교 전자계산학과(이학사)
- 1993년 2월 : 단국대학교 전산통계학과대학원 석사(이학석사)
- 2003년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사(공학박사)
- 1997년 3월 ~ 현재 : 백석문화대학교 컴퓨터공학부 교수
- 관심분야 : 네트워크 보안, IoT 보안
- E-Mail : sylee@bscu.ac.kr