대량 스팸메일 발송 방지를 위한 SMS 기반 DomainKey 방식의 송신자 인증 기법

Sender Authentication Mechanism based on DomainKey with SMS for Spam Mail Sending Protection

이형우
한신대학교 컴퓨터정보소프트웨어학부

Hyung-Woo Lee(hwlee@hs.ac.kr)

요약

전자우편은 인터넷을 이용하는 사용자들에게 중요한 커뮤니케이션의 역할을 담당하고 있다. 하지만, 원하지 않는 광고 정보를 포함한 스팸 메일, 악성코드 형태를 포함한 바이러스 메일 등 대부분이 불필요한 자료들로 인해 전자우편이 가지는 본연의 의미와는 무색하게 사용되고 있어 근본적인 측면에서 스팸 메일의 발송을 방지할 수 있는 방안에 대한 연구가 시급하다. 본 연구에서 전자우편 발송자는 SMS(Short Message Service) 방식으로 별도의 비밀 정보를 전달받고 이를 통해 DomainKey 방식에서 사용하는 개인키/공개키 쌍을 생성하도록 하였으며 기존의 PGP 방식과도 접목하여 전자우편 송신자에 대한 인증 및 메시지에 대한 암복호화 기능을 수행하는 기법을 제안한다. 제안한 기법은 메일 발송 과정에서 발신자에 대한 인증 과정을 수행하므로 스팸 메일의 발송을 방지할 수 있는 기법이다.

■ 중심어 : | 스팸메일 | 송신자 인증 | SMS | 도메인키 방식 | PGP 기법 |

Abstract

Although E-mail system is considered as a most important communication media, 'Spam' is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Therefore advanced anti-spam techniques are required to basically reduce its transmission volume on sender mail server or MTA, etc. In this study, we propose a new sender authentication model with encryption function based on modified DomainKey with SMS for Spam mail protection. From the SMS message, we can get secret information used for verification of its real sender on e-mail message. And by distributing this secret information with SMS like out-of-band channel, we can also combine proposed modules with existing PGP scheme for secure e-mail generation and authentication steps. Proposed scheme provide enhanced authentication function and security on Spam mail protection function because it is a 'dual mode' authentication mechanism.

■ keyword : | Spam Mail | Sender Authentication | SMS | DomainKey | PGP |

* 본 논문은 2005년도 한국학술진흥재단 지역대학우수과학자지원사업의 지원에 의해 연구되었습니다. (KRF-2005-202-D00487)

접수번호 : #070131-001
접수일자 : 2007년 01월 31일
심사완료일 : 2007년 02월 22일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

I. 서 론

현재 우리는 인터넷을 통한 정보화 사회를 실감하고 있으며, 잠시도 인터넷을 이용하지 않고서는 정보화 사회에서 경쟁우위를 차지할 수 없다. 인터넷을 통해 개인 정보 유통 체계로 가장 많이 사용되는 것 중에 하나는 전자메일(e-mail) 시스템이다. 웹을 통한 메일 시스템인 경우 1인 1 ID를 가지고 있을 정도로 국내 메일 시스템의 활용도는 매우 높다. 그러나, 근래 메일을 통한 악성 바이러스 코드가 유포되어 해킹/바이러스의 감염 경로로 활용되고 있을 뿐만 아니라, 불법 정보 유통, 성인 정보의 유통 경로로 활용되고 있어 이에 대한 '근본적인 스팸 메일 차단 및 능동적 대응 기술 개발'이 시급하다.

스팸 메일이 매년 200% 이상으로 증가되고 있으며, 형태 또한 갈수록 지능화되고 있다. 이와 같이 폭증하는 스팸 메일로 인해 기업과 사회가 치르는 사회적/경제적 비용도 엄청나게 증가하고 있다. 최근 조사한 자료에 의하면 스팸 메일로 인해 전체 국민들이 입는 사회적/경제적 손실이 연간 2조 6451억원에 이른다고 한다[1]. 하루에 유통되는 스팸 메일의 건수가 9억 1504만 통이며, 1인당 연간 44시간을 스팸 메일을 지우는데 허비하는 것으로 나타났다. 또 기업에서는 네트워크상의 유해 트래픽 유발로 네트워크/메일서버의 속도 및 성능이 저하되고 있으며, 이런 문제점들을 해결하기 위해 매년 수억 원 씩의 비용이 불필요한 서버장치를 추가로 구입하는데 쓰여지고 있는 현실이다. 스팸 메일을 퇴치하기 위해 현재 가장 많이 사용하는 방식은 Filtering 방식[3]을 사용하고 있으나, 이 방식은 스팸을 특정 단어나 문구로 규정하기 때문에 스팸 오경보와 같은 필터링 오류발생 또는 스팸 메일의 낮은 탐지률 등과 같이 아직까지 해결되지 않는 문제로 남아있다.

현재까지 제시되고 있는 대부분의 스팸 대응 기술은 이미 스팸 메일이 발송된 이후에 특정 단어 또는 패턴을 중심으로 사후에 필터링하는 방식을 사용하고 있다. 따라서 기존의 메일 수신자 측면에서의 필터링 기반 스팸 메일 차단은 근본적인 스팸 차단 기술이라고 할 수 없으며 개선된 스팸 차단 기술 개발이 필요한 시점이다.

이와 같이 기존 스팸 메일 방지 기법의 취약점 해결하기 위해서는 송신자의 메일에 자신의 서명을 넣어 송신자에 대한 인증 기능을 제공하고 메일 메시지에 대한 암호화를 통해 기밀성/비밀성을 제공하는 방법이 필요하다[4].

이에 본 연구에서는 스팸 메일에 대한 발신 단계에서 스팸과 관련된 송신 과정을 차단하는 기능을 제공하기 위해 메일 발신지에 대한 확인/검증 기능을 제공하고 메시지에 대한 무결성을 보장하면서도 수신자 측면에서 송신자에 대한 확인 기능을 제공하고자 한다.

본 연구에서 개발한 기술을 이용할 경우 스팸 메일에 대한 송신과정에서의 확인/검증 과정을 수행하게 되므로 스팸에 해당하는 메시지 전송 자체를 감소시킬 수 있을 뿐만 아니라, 스팸을 통한 악성 바이러스 전송 등도 차단할 수 있는 효과를 제공할 수 있을 것으로 기대된다.

본 논문의 I장 서론은 스팸 메일의 실태에 대해 설명하고 본문 II장 관련연구 에서는 기존의 스팸 차단 기술과 그 기술들의 문제점을 지적한다. III장 제안 모델 에서는 제안하는 모델에 대해 설명 및 필요성과 제안 시스템으로 인한 스팸 차단 효과에 대해 설명한다. IV장은 기존 시스템과의 비교분석을 통해 제안 시스템의 특징을 설명한다. V장 결론에서는 연구결과의 정리와 향후 연구 과제에 대해 설명한다.

II. 관련연구

1. 스팸메일

스팸 메일이란 인터넷 공동체에서의 원하지 않는 전자메일 (UBE-Unsolicited Bulk E-mail), 원하지 않는 상업적 전자메일 (UCE- Unsolicited Commercial E-mail), 무차별적인 폭탄 메일 등을 의미하는데, 최근 들어 스팸 메일은 상업적 목적의 마케팅 수단으로 이용되고 있다. 이렇게 상업적인 목적으로 메일이 사용되는 이유는 인터넷 마케팅의 특징인 투자비용 대비 효과측면에서 기존의 오프라인 광고보다 월등한 효과를 보이기 때문이다. 이로 인해 소비자들의 피해는 날로 극심

해지고 있다.

현재의 SMTP[2] 기반 메일 송수신 구조는 다음 그림과 같다. 송신자는 메일 클라이언트를 통해 메시지를 작성하면 MTA[3]에 의해 메일은 전송되며, 수신자는 마찬가지로 MTA로부터 SMTP 프로토콜에 기반하에 메시지를 전송받는 방식이다.

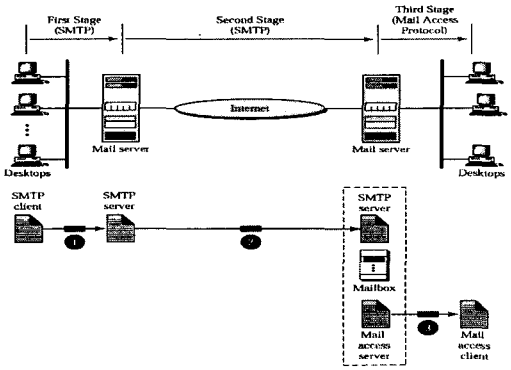

그림 1. SMTP 프로토콜 작동방식

이 과정에서 크게 아래와 같은 이유로 인해 스팸메일이 발생하게 된다.

- 대량의 광고성 메일 수신
- SMTP 발신자 확인 기능 미비
- 임의의 발신자에 의해 메일 발송
- 메일 발신자에 대한 인증 기능 미비

따라서 현재까지는 대량의 광고성 메일이 임의의 수신자에게 발송되는 과정에서 메일에 대한 필터링 기법 등을 이용하여 스팸메일에 대한 대응을 수행하였다. 하지만 이는 근본적인 대응방안이 되지 못하고 있다.

스팸메일이 발생하는 근본적인 이유는 임의의 발신자에 의해 손쉽게 메일을 전송한다는 것이다. 따라서 SMTP 프로토콜에서의 발신자 인증 및 프로토콜에서의 보안 강화 방법을 토해 능동적으로 스팸메일에 대해 대응할 수 있다. 이와 관련하여 기존의 스팸 메일 방지 기법에 대해 살펴보면 다음과 같다.

2. 기존 스팸방지 기법

2.1 SPF(Sender Policy Framework)

SPF[12] 기술은 메일의 헤더를 보고 실제 해당 메일 서버에서 보내진 것인지를 판단하여 불법적 스팸 메일에 대한 수신을 막는 방법이다.

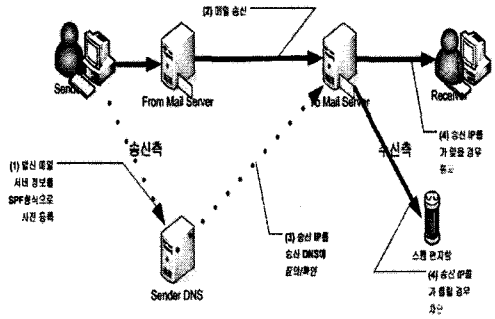

그림 2. SPF 기법 작동방식

예를 들어 메일의 From 헤더를 foo@spammer.com 이라고 적혀있으면 spammer. com을 관리하는 DNS 서버를 통해서 해당 메일에 실제로 설정된 spammer.com 의 IP와 수신된 메일 헤더의 IP를 비교해서 만일 다르면 수신을 거부하게 된다. 즉, 실제로 hanmail.net에서 보내지 않은 메일주소에 @hanmail.net와 같이 변경하여 메일을 발송할 경우 이를 SPF에서는 필터링하게 된다.

2.2 RBL(Real-time Blocking List)

RBL 기법[15]은 실시간으로 차단 IP를 탐지하고 그것을 공개하는 방법을 사용한다. 표면적으로 보면 단순한 IP 리스트에 불과한데, 그 종류와 목표에 따라 매우 다양할 수 있다.

- 실시간으로 PA일 릴레이가 가능한 IP주소만을 수집하고 공개하는 DB
- 실시간으로 해킹에 도용될 수 있는 Proxy의 IP 주소만을 수집하고 공개하는 DB
- 실시간으로 불량소프트웨어에 감염된 좀비 PC의 주소만을 수집하고 공개하는 DB

이와 같은 방식으로 다양한 형태의 데이터베이스가 존재할 수 있으며, 그것들을 통칭해서 Black List 데이터베이스라고 한다. 통상적으로 RBL이라고 함은, 공통적으로 DNS 룩업을 통해서 특정 IP의 불량 여부를 판단할 수 있는 데이터베이스 기반 스팸 차단 기법을 의미한다.

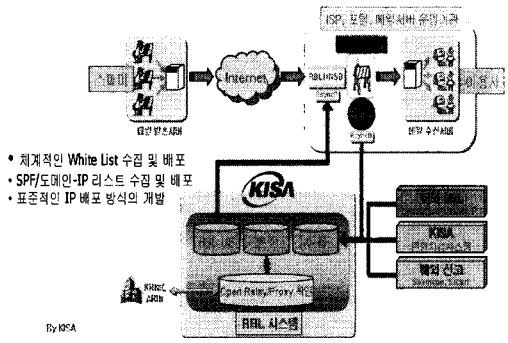

그림 3. RBL 기법 작동방식 [출처 : KISA]

2.3 C/R(Challenge/Response) 필터링

C/R 필터링[6] 시스템은 송신자의 이메일 Challenge가 포함된 이메일 메시지에 응답하는 스팸 필터 방식이다. Response된 사용자는 다음부터는 정상적으로 메일 서비스를 받을 수 있다. 그러나 그 응답은 메일 Server 관리자에게 이루어지는 방식으로 메일 관리자의 오류로 인해 Sender의 인증이 다른 사람에게 Response될 수 있다. 그리고 From 헤어의 노출로 송신자의 정보가 스푸핑되는 취약점을 가지고 있다.

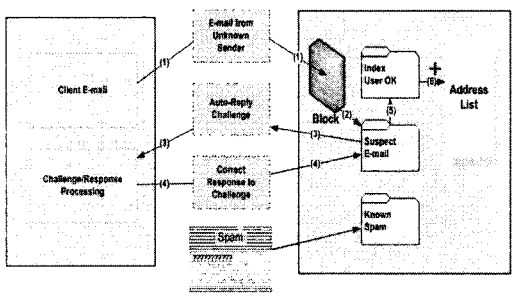

그림 4. C/R Filtering 시스템 구성도

3. 기존 스팸방지 시스템의 취약점 및 해결방법

기존의 스팸방지 시스템에도 문제점을 가지고 있다. 발신 메일 서버정보를 SPF에 사전 등록을 해야하는 번거로움, 그리고 가장 큰 문제점은 등록 및 인증되지 않은 발신 메일 서버로부터 오는 정상 메일이 차단되는 2차 피해가 심각한 문제점이다. 또 전자 메일 마케팅이 주요 홍보수단으로 생각하는 중소기업의 마케팅 활로 차단이라는 문제점 또한 가지고 있다.

기존의 필터링 방식에 의한 스팸 대응 기술은 지능화되고 복잡한 형태로 발전하는 스팸 메일 발송에 수동적/제한적으로 대응한다는 단점이 발생한다.

근본적인 측면에서 고찰해 본다면 기존 SMTP 프로토콜 헤더 정보에서는 손쉽게 스패머에 의해 헤더 정보 변경 및 대량 재전송이 가능하다. 메일 헤더 정보에서 전송자 주소 및 제목 등에 대해 스푸핑하여 전송하더라도 기존의 SMTP 프로토콜에서는 이를 검증하지 못하고 있다. 이는 기존의 SMTP 프로토콜에서는 불법 스팸 전송을 사전에 방지할 수 있는 보안 및 안전한 발송/인증 메커니즘이 전무하기 때문이다. 결국, 기존 SMTP 프로토콜에서의 취약점을 개선하기 위한 개선된 기법에 대한 연구가 필요하다.

III. 기존 DomainKey 기법 분석

'DomainKey'란 메일 서비스가 발송자의 도메인과 보내진 메시지의 일관성을 검증할 수 있도록 하기 위해 제시되었다. 도메인 검증이 가능해지면 메일의 '보내는 사람' 필드에 입력된 사람의 도메인을 확인하여 그 메일이 위조된 것인지 여부를 판단한다. 위조된 것이라면 스팸으로 판단하여 사용자에게 해를 끼치지 않도록 버려지고, 위조가 아니라면 그 도메인은 검증된 것이므로 스팸센터 및 타 메일 서비스들, 또한 다른 유저들에게까지 유효한 도메인으로 알려지게 된다[7].

1. DomainKey 전송서버 작동방식

도메인 키를 통해 메일을 인증하는 데에는 두 가지 단계가 있다. 준비 단계 : 도메인 소유자는 발신되는 모

든 메시지에 사용되는 Public/Private 키를 생성한다. Public Key는 DNS에서 활성화되고 Private Key는 도메인 키가 적용된 메일 발송 서버에서 생성/관리한다.

인증 단계 : 메일을 전송하는 과정에서 메일 시스템은 저장된 Private Key를 이용하여 메시지에 대한 디지털 서명(Digital signature)을 생성한다. 이제 이 서명은 메시지 헤더에 남아있고, 메시지는 수신자의 메일 서버로 전송된다.

2. DomainKey 수신서버 작동방식

인증된 메일을 확인하기 위해 세가지 단계를 수행한다.

- **준비 단계** : 도메인 키가 적용된 메일 수신 시스템은 메시지 헤더로부터 디지털 서명과 'From'의 도메인을 추출하고, DNS로부터 'From'의 도메인의 Public Key를 내려받는다.
- **확인 단계** : DNS로부터 받은 Public Key는 메시지 헤더의 디지털 서명이 Public Key와 매치되는 Private Key로부터 만들어졌는지 확인하는데 사용된다. 이것은 메일이 실제로 'From'의 도메인 승인 후 보내졌는지, 그리고 메일 헤더와 내용이 전송 중에 수정되지 않았는지 여부를 증명하게 된다.
- **배달 과정** : 메일 수신 시스템은 디지털 서명 테스트의 결과에 따라 자체적인 방법을 수행한다. 만약 도메인이 확인되었고 다른 스팸 테스트를 통과했다면 메일은 사용자의 수신함에 배달된다. 만약 서명이 확인되는데 실패하거나 테스트 자체가 없었다면 이 메일은 전달되지 않거나 스팸 편지함으로 전송된다.

3. DomainKey 기반 인증 기법의 문제점

DomainKey 방식에서는 해당 MTA를 설치해야 하고 MTA에 대한 키 설정 및 분배 과정을 지원해야 한다는 문제점이 있다.

DomainKey에서는 Private Key를 사용하여 메시지에 대한 서명을 생성하지만 전체 내용에 대한 서명이 아니기 때문에 결국에는 생성된 메시지에 대한 재전송 등이 가능하다. 따라서 DomainKey 방식에서 문제점이 되는 재전송 문제를 방지하기 위해서는 각 메시지마다 각기 다른 Private/Public Key 쌍을 적용해야 한다. 또한 DomainKey는 메시지 전송 과정에서 메일의 내용이 변경되므로 첨가된 디지털 서명값은 더 이상 검증에 활용할 수 없는 상황이 되기도 한다. 따라서 DomainKey에서는 재서명(re-sign) 과정을 수행하거나 기존의 SPF[12] 등의 기법과 연계하는 방법을 쓰고 있다.

하지만 앞에서 살펴본 바와 같이 SPF 역시 발신자의 IP 주소 값을 중심으로 메일 발신자의 적법성을 판별하는 방식이지만, 만일 IP 스푸핑에 의해 메일을 발송할 경우 이것 역시 문제점을 지니고 있다.

따라서 본 연구에서는 MTA를 중심으로 기존의 DomainKey에서의 Public/Private Key 생성 및 키관리 관리구조의 안전성/효율성을 높이고 재전송 및 전달 과정에 손쉽게 대응하기 위해 SMS 시스템을 통한 새로운 발신자 인증 기법을 개발하였다.

IV. 제안한 기법

본 논문에서는 기존의 스팸방지 시스템의 취약점을 보완하기 위하여 SMS(Short Message Service)를 이용해 메일 서버와 Sender간의 대칭키를 공유하므로 메시지의 암호화와 공개키 방식을 사용해 Sender의 인증을 받는 모델을 제안한다.

본 기법에서 사용한 기호는 다음과 같다.

KS : 관용암호에서 사용하는 세션키
KRa : 공개키 암호 방식에서 사용되는 사용자 A의 개인키
KUa : 공개키 암호 방식에서 사용되는 사용자 A의 공개키
EP : 공개키 암호방식을 이용한 암호화
DP : 공개키 암호방식을 이용한 복호화
EC : 관용암호방식을 이용한 암호화
DC : 관용암호방식을 이용한 복호화
H : 해쉬 함수
|| : 연접
Z : ZIP 알고리즘을 이용한 압축

1. 제안한 기법의 특징

DomainKey에서는 RSA 공개키 암호 알고리즘을 기반으로 Public/Private Key를 생성하고 이를 이용하여 메시지에 대한 서명/확인 과정을 수행하게 된다.

이와 같은 방식은 기존의 PGP 기반 전자우편 보안 프로토콜과 유사한 방식이라는 것을 알 수 있다. PGP 기법에서 사용하는 주요 기법은 다음과 같다.

- 디지털 서명
  - SHA-1[8]을 사용하여 해쉬코드 생성
  - DSS 또는 RSA를 사용하여 메시지 다이제스트에 대한 서명

- 메시지 암호화
  - CAST, IDEA[9], 3DES[8], D-H, RSA 사용

- 압축 및 호환성 제공
  - 전장 및 전송을 위해 ZIP으로 암축
  - 암호화된 메시지를 Base-64 코드 적용 후에 ASCII 문자열로 변환

PGP 기법인 경우 Private Key 및 Public Key에 대해서는 Key Ring 개념을 적용하여 사용자가 사용할 수 있도록 한다. 사용자가 소유한 키쌍과 함께 다른 사람의 Public Key 등을 저장하기 위한 구조를 가지고 있다.

- 개인키 링
  - 사용자 Pi의 ID나 키 ID로서 색인화
  - 키쌍을 생성/소유한 사용자 시스템에 저장
  - 개인키의 안전을 위하여 암호화하여 저장
  - EH(Pi)[KRi]

- 공개키 링
  - 사용자 ID나 키 ID로서 색인화

이와 같은 기반 구조를 이용하여 메일 메시지에 대한 인증 및 암호화 과정을 지원하는 과정은 아래 그림과 같다.

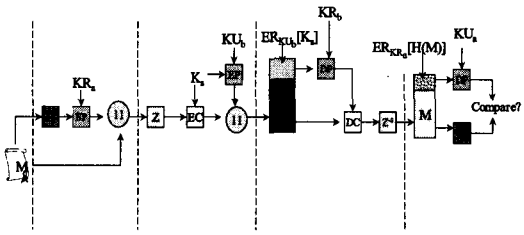

그림 5. 기존의 e-mail 인증/암호화 구조

하지만 attack으로부터 공개키를 보호하는 일이 가장 어려운 문제이다. 최근 이에 대해 바이오 인증 등의 기법까지 적용하는 등 다양한 기법에 대한 연구가 수행되고 있다.

DomainKey 방식 역시 MTA를 통해 메일 메시지에 대한 서명을 수행한 후에 전달하는 과정에서 각각의 MTA에는 공개키/개인키 쌍이 생성되어야 하고, 수신 MTA 입장에서는 송신자의 공개키를 받아서 확인하는 과정을 수행하기 때문에 결국에는 PGP[12][16] 방식과 유사한 키 링 구조를 유지/관리하여야 한다는 문제점이 있다.

따라서 본 연구에서는 SMS 시스템이 갖고 있는 핸드폰 기반 개인 확인 기능 및 무선 시스템을 통한 사용자 검증 기능을 이용하면서도 SMS 시스템을 통해 DomainKey 및 PGP 기반 메일 암호/인증에서 사용되는 비밀 정보를 송신하는 구조를 적용하여 좀더 효율적이면서도 강화된 인증 구조를 제시하였다.

2. 제안 모델

기존의 스팸방지 시스템은 송신자 IP, 그리고 필터링 기법들을 이용해 이루어 졌다. 그러나 이런 방식들은 II 장에서 설명했듯이 많은 문제점을 가지고 있다. 가장 큰 문제는 Sender의 인증 과정이 없다는 것이다.

SMS를 이용한 Sender Verification은 송신자의 인증을 통해 스팸 메일을 차단할 수 있다는 것에 포커스를 맞추고 있다. 몇해 전부터 1인 1전화 시대를 이룬 현 시점에 핸드폰의 문자서비스는 많은 인증 절차에 이용되고 있다. 예를 들면 소액결제는 핸드폰의 요금 부과로 이루어지는 경우도 있고, 전자상거래시 신용카드 결제에 핸드폰 인증을 사용하는 방식이 두드러지게 증가

했다. 이는 핸드폰의 보편성을 이용해 개인의 인증을 하기 위함이다.

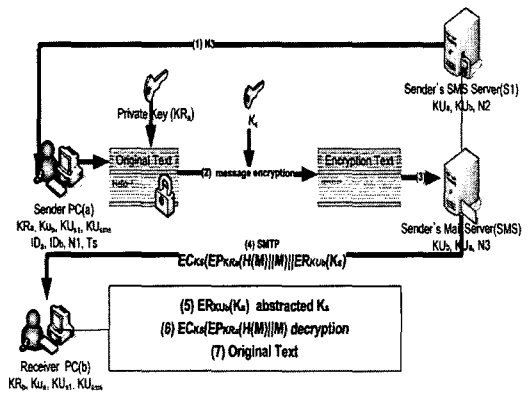

그림 6. SMS를 이용한 제안 시스템 구성도

[그림 6]은 본 논문의 전체적인 구성도이다. Sender는 메일을 보내기 위해 POP3, IMAP4, WebMail에 접속을 한다[10]. 그 이후의 과정은 다음과 같다.

송신자가 메일을 보내기 위해 Application에 접속했을 때 Sender's SMS Server로부터 메시지 암호화 과정에서 Ks를 생성과 관련되는 난수 정보를 송신자 핸드폰의 문자 서비스로 전송받는다. 이때 메일 서버 가입 시 입력된 핸드폰 정보를 이용한다.

송신자는 개인키를 이용해 자신의 메일에 서명을 한다. 이때 SMS로부터 부여받은 난수 정보를 생성된 Ks 이용해 메일의 메시지 암호화도 함께 이루어진다. 송신자의 메일은 Mail Server로 전송된다. SMTP에 의해서 수신자 메일서버로 전송이 된다. 이때 암호화된 메시지는 수신자의 개인키로 Ks를 알 수 있다. 그러므로 암호화된 메시지를 복호화 된다. 수신자는 송신자의 공개키를 이용해 송신자 인증을 절차를 밟는다. 앞의 절차가 정상적으로 이루어 졌을 경우 수신자는 Original Text를 수신한다.

3. 키 생성 및 분배 과정

본 논문은 PGP[11]의 알고리즘을 이용한 스팸 메일 방지 기법에서 효율적인 키 분배를 위해 SMS 서버를 사용하였다. 그리고 송신자 인증에 메시지 암호화 기법을 더한 보다 안전한 스팸메일 방지 시스템이다.

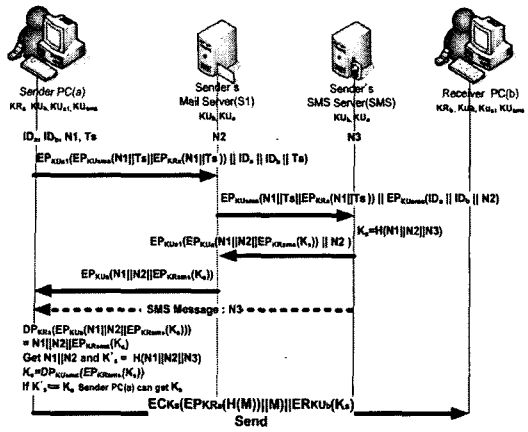

그림 7. 제안한 기법의 키생성/분배 방식

본 논문 키 분배 시나리오에서 a는 송신자 b는 수신자를 의미한다. 비밀키 KRx(x=a, b), 공개키 KUx(x=a, b), 공개키 암호화 방식(RSA)[8]을 이용한 메시지 암호화 EP, 복호화 DP로 정의할 경우 다음과 같은 과정을 수행한다.

관용 암호화 과정에서 사용하는 세션키 Ks, 관용암호화 방식을 이용한 암호화 EC, 복호화 DC. 그리고 Sender's 및 Receiver's SMS Server에는 모든 ISP업체 및 개인 메일 서버 사용자의 공개키를 가지고 있다고 가정한다.

Sender가 가입된 SMS Server에서는 메일서버 및 사용자로부터 전달받은 정보를 토대로 Ks를 생성하고 송신자의 핸드폰에 관련된 정보를 SMS 메시지로 전송해준다. 구체적인 과정은 아래와 같다.

- 1단계 : 사용자 a는 기본 정보를 생성
  - IDa : 송신자에 대한 정보(메일주소, 이름 및 핸드폰 번호) 등으로 구성됨
  - IDb : 수신자에 대한 정보
  - N1 : 임의의 난수값을 송신자가 생성
  - Ts : 사용 기간에 대한 정보

- 2단계 : 사용자 a는 메일서버에 요청
  - EPKUsms(N1 ‖ Ts ‖ EPKRa(N1 ‖ Ts)) 생성

- 앞에서 생성된 값을 IDa, IDb 및 Ts와 연접한 후에 메일서버의 공개키로 암호화하여 전송
  $EP_{KUsl}(EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts)) \| IDa \| IDb \| Ts)$

• 3단계 : 메일서버는 SMS 서버에 키생성요청
- 메일서버는 사용자로부터 수신한 값을 복호화하고 IDa, IDb 및 Ts 값을 기록함
- 이때 Ts 값은 키 사용 기간을 의미하기 때문에 해당되는 시간 동안에만 사용하게 됨
- 이제 메일서버는 임의의 난수 N2를 생성
- 생성된 값과 사용자로부터 받은 IDa, IDb 값을 이용하여 SMS 서버에게 아래와 같이 키 생성을 요청함
  $EP_{KUsms}(N1 \| Ts \| EP_{KRa}(N1 \| Ts)) \| EP_{KUsms}(IDa \| IDb \| N2)$

• 4단계 : SMS 서버는 세션키 Ks를 생성함
- SMS 서버는 메일서버로부터 수신된 값을 복호화하고, 사용자에 대한 서명에 대한 검증 과정을 수행하여 값을 복호화하고 키 생성 절차를 수행
  DPKRsms(EPKUsms(N1 ‖ Ts ‖ EPKRa(N1 ‖ Ts)))= N1 ‖ Ts ‖ EPKRa(N1 ‖ Ts)
  DPKUa(EPKRa(N1 ‖ Ts) = N1 ‖ Ts
  DPKRsms(EPKUsms(IDa ‖ IDb ‖ N2)) = IDa ‖ IDb ‖ N2
- SMS 서버는 임의의 난수 N3를 생성하고 다음과 같이 세션키 Ks를 생성함
  Ks=H (N1 ‖ N2 ‖ N3)

• 5단계 : SMS 서버는 세션키 Ks 관련 정보 등을 메일서버와 사용자에게 전송함
- SMS 서버는 메일서버로부터 받은 N2 값을 이용하여 확인 응답 절차로 아래와 같은 메시지를 생성하여 전송함
  $EP_{KUsl}(EP_{KUa}(N1 \| N2 \| EP_{KRsms}(Ks)) \| N2)$
- 생성된 정보에는 N1 및 N2 값을 통해 SMS 서버가 메일서버로 확인 응답을 전송하게 되며 이때 Ks 정보는 EPKUa(N1 ‖ N2 ‖ EPKRsms(Ks)) 형태로 사용자 A의 공개키로 암호화하여 사용자만이 복호화할 수 있도록 하고 메일서버는 N2 값을 통해서 응답에 대해 확인하게 됨
- 또한 SMS 서버는 임의의 난수 N3에 대해서 핸드폰의 SMS 메시지 형태로 사용자의 핸드폰에 발신하게 됨

• 6단계 : 메일서버는 SMS 서버로부터 수신된 메시지에 대해서 사용자에게 전달함
- 메일서버는 SMS 서버로부터 전달받은 메시지에 대해 복호화된 내용을 다시 사용자에게 전달함
  $EP_{KUa}(N1 \| N2 \| EP_{KRsms}(Ks))$

• 7단계 : 사용자는 메일서버와 SMS 서버로부터 수신된 메시지에 대해서 키 확인 과정을 수행하고 메일에 대한 전송 과정을 수행
- 아래와 같은 검증 과정을 통해 Ks 값을 확인함
  $DP_{KRa}(EP_{KUa}(N1 \| N2 \| EP_{KRsms}(Ks)))$
  $= N1 \| N2 \| EP_{KRsms}(Ks)$
  Get N1 ‖ N2 and K's = H(N1 ‖ N2 ‖ N3)
  $Ks=DP_{KUsms}(EP_{KRsms}(Ks))$
  If K's== Ks Sender PC(a) gets Ks

이제 사용자는 수신자에게 Ks를 이용하여 메일 메시지 M을 전송하고 동시에 인증/암호화 기능을 이용한 안전한 메일 전송 과정을 수행할 수 있다.

4. 송신자 인증 및 암복호화 과정

송신자는 자신이 보내려하는 수신자의 공개키를 얻을 수 있으며 자신의 개인 키는 이미 안전한 곳에 저장되어 있다. 그리고 Ks는 SMS 서버로부터 일정 시간동안 사용할 수 있도록 부여 받았다. 이 과정에서 SMS 메시지 방식을 통해 전달받았기 때문에 패킷 스니핑 등의 공격 등에 안전하다고 할 수 있다. H(M)를 통해 메시지를 해쉬한 값을 송신자의 개인키를 이용해 인증을 위해 암호화 하고 $EP_{KRa}(H(M))$ 원래 메시지와 연접한다($EP_{KRa}(H(M)) \| M$). 이 값은 다시 메시지 암호화를 위해 관용암호방식을 이용해 Ks를 세션키 값으로 사용해 메시지 암호화 한다($EC_{Ks}(EP_{KRa}(H(M)) \| M)$). 그러

나 수신자는 Ks를 모르므로 수신자의 공개키를 이용해 Ks를 암호화하고 $EC_{Ks}(EP_{KRa}(H(M)) \| M)$과 연접한다.

$$EC_{Ks}(EP_{KRa}(H(M)) \| M) \| ER_{KUb}(Ks)$$

이 값은 최종적으로 수신자에게 전달된다.

수신자는 자신의 개인키와 송신자의 공개키를 알고 있다. 우선 Ks를 알기 위해 자신의 개인키를 이용해 $ER_{KUb}(Ks)$를 복호화 한다. 복호화로 알게된 Ks값을 이용해 암호화된 메시지를 복호화 한다.

$EC_{Ks}(EP_{KRa}(H(M)) \| M)$ 복호화된 메시지는 송신자 인증을 위해 송신자의 공개키를 가지고 $EP_{KRa}(H(M))$를 복호화 한다. 그렇게해서 나온 H(M)과 연접했던 M을 해쉬한 H(M)과 비교해 송신자를 인증한다. 위와 같은 과정은 기존의 DomainKey 및 PGP 방식과 유사한 과정을 수행하게 된다.

V. 안전성 평가 및 비교분석

1. 제안 기법의 안전성 평가

기존의 DomainKey 기법인 경우 MTA를 통해 전송하고자 하는 메일 메시지에 대한 서명을 수행한 후에 수신자의 MTA로 전달한다. 이때 각각의 MTA에는 공개키/개인키 쌍이 생성되어야 하고, 수신 MTA 입장에서는 송신자의 공개키를 받아서 확인하는 과정을 수행하기 때문에 결국에는 안전한 키 분배 및 관리 구조와 접목되어야 한다.

본 연구에서 제시한 기법인 경우 기존의 PGP 및 DomainKey 기법에서와 같이 공개키/개인키 쌍을 이용한 공개키 암호 기법을 적용하였기 때문에 메일 메시지에 대한 무결성, 기밀성 및 인증 기능을 제공하게 된다.

특히 본 연구에서 제시한 기법인 경우 SMS 시스템이 갖고 있는 핸드폰 기반 개인 확인 기능을 이용하여 기존의 TCP/IP 기반 네트워크 트래픽 이외에 무선 핸드폰 메시지를 통해 키와 관련된 값을 전송하는 이중 인증 시스템을 구축하였기 때문에 기존의 PGP 및 DomainKey 기법보다도 더욱더 강화된 전자우편 보안 및 발신자 인증 구조를 제공할 수 있었다.

Ethereal 등의 패킷 스니핑 툴 등을 통해 전자우편 메시지에 대해 모니터링이 가능하다. 본 연구에서 제시한 기법은 기존의 TCP/IP 기반의 네트워크 환경만을 이용하지 않고 핸드폰과 같이 분리된 무선망을 복합적으로 접목하였기 때문에 기존의 기법보다도 안전성을 높일 수 있다는 장점이 있다. 세션키 Ks에 대해서는 SHA-1 또는 MD5 등의 해쉬 함수를 이용하기 때문에 일방향적인 특성을 보이고 있다. 따라서Ks 값의 안전성을 해쉬함수의 안전성에 기초하고 있기 때문에 본 연구에서 제시한 기법은 기존의 DomainKey 및 PGP 기법보다 향상된 인증 및 보안 기능을 제공한다.

2. 기존 기법과의 비교 분석

본 연구에서 제안한 모델은 메일 메시지 암호화 와 송신자 인증의 이중 암호화로 더욱더 강력한 보안 시스템을 구축하고 있다. 그리고 메시지 암호화를 위한 Ks 대칭키를 SMS Server로부터 안전하게 전송 받는다. [표 1]은 기존의 시스템과 제안 시스템의 특징들을 비교 분석한 내용이다. 비교 결과 제안한 기법은 기존의 기법보다 개선된 결과를 제공한다.

제안한 기법은 발신자 인증 기법을 통해 스팸 메일에 대한 발생을 억제하는 방식으로, 메일 메시지에 대한 암호화 기능을 제공하면서도 무결성 및 안전성 기능

표 1. 기존 기법과의 안전성 및 성능 비교 평가

특성 / 기법	스팸차단방식	발신자 인증기능	메일 암호화	무결성 제공	안전성	키분배 기능	비고
Filtering기법[3]	메일내용필터링	×	×	×	×	×	메일컨텐츠필터링방식
SPF[12]	IP주소기반	△	×	×	▽	×	DNS검색방식
DomainKey[13]	발신자인증	△	◇	◇	◇	×	공개키암호화방식
PGP[14]	해당사항 없음	◇	△	△	△	O	키링방식
제안한 기법	발신자 인증	△	△	△	△	O	이중인증

O: A ×: N/A △:good ◇:moderate ▽:bad

을 제공한다. 또한 핸드폰 등과 연계된 키 분배 기능을 포함하고 있어서 최근 문제가 되고 있는 유선 트래픽에 대한 스니핑 공격 등에 안전한 이중인증(dual authentication) 기능을 제공한다.

VI. 결론

본 연구에서 제안한 모델은 핸드폰의 보급으로 그동안의 키 분배 과정에서의 불안전성을 SMS를 이용한 키 분배로 보완해 메시지 암호화와 송신자 인증 과정에서 공개키 기반 알고리즘의 키를 안전하게 송수신자에게 전달하는 모델을 제안 했다. SMS의 키 분배는 기존에 결제 시스템에서도 그 안전성과 보안성을 검증받은 상태이다. 그리고 기존의 단순한 IP비교와 필터링 기술에서 벗어나 핸드폰을 이용해 송신자의 인증을 할 수 있는 기법을 제안하였고 발신자 인증 및 메일에 대한 안정성 기능을 통시에 제공할 수 있었다.

앞으로 본 연구를 토대로 메일 시스템에서의 인증 과정 및 웹 기반 인증 시스템에 SMS 기반 이중 인증 체계를 접목하여 보다 다양한 방식으로 발전시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] http://www.spambreaker.co.kr/loss_expense.html

[2] http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[3] N. Tran, "Anti spamming - How to filter unsolicited e-mail on your mail server," Dec. 2001.

[4] P. Cocca, "Email Security Threats," SANS Institute 2005, Sep. 2004.

[5] P. Fisher, "Creating a Hardened Internet SMTP Gateway in Exchange 2003," Feb. 2005.

[6] http://www.joewein.de/sw/spam-challenge-response.htm

[7] http://kr.antispam.yahoo.com/domainkeys

[8] Wade Trappe, Lawrence C. Washington, "Introduction to CRYPTOGRAPHY with Coding Theory," Prentice Hall, 2002.

[9] 이임영, 송유진, *현대 암호화*, 생능출판사, 1999(2).

[10] 이형우, *스팸 차단 기술동향*, 한국정보보호진흥원 보고서, 2006(4).

[11] J. D. Dyson, *Public Key Cryptography & PGP*, 1999.

[12] http://www.openspf.org/

[13] http://antispam.yahoo.com/domainkeys

[14] http://www.pgpi.org/

[15] http://www.email-policy.com/Spam-black-lists.htm

저 자 소 개

이 형 우(Hyung-Woo Lee) 정회원

- 1994년 2월 : 고려대학교 컴퓨터학과 (이학학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 1999년 3월 ~ 2003년 2월 : 천안대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터정보소프트웨어학부 교수

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 컨텐츠 보호