SW 형태의 보안카드와 PGP 기반 안전한 E-mail 송신자 인증 기법

이형우†

요 약

전자메일(e-mail)시스템은 인터넷을 통해 개인의 정보를 전달하는 매체로 가장 많이 사용된다. 그러나 송신자의 위변조 및 다수 사용자에게 메일을 전송하는 기법 등을 이용한 전자메일의 역기능 또한 늘어나고 있는 추세이다. 본 논문에서는 송신자의 위변조를 막기 위해 보안카드를 이용한 송신자 인증 기법을 제안 한다. 송신자는 메일 전송시 보안카드의 특정 코드번호를 송신자의 메일 서버로부터 요청 받는다. 송신자는 메일 서버로부터 요청 받은 코드 번호를 입력해 송신자 인증 절차를 거친 후 세션키를 생성한다. 생성된 세션키는 송신자의 서명 및 메시지를 안전하게 전송할 수 있는 암호화 키로 사용된다. 제안한 기법은 송신자 인증과 송신자 서명 및 메시지 암호화를 통해 기존의 스팸 방지 기법 보다 더욱 안전한 인증 구조를 제공한다.

키워드 : 스팸메일, 보안카드, 전자우편 송신자 인증, PGP

Sender Authentication Mechanism based on SW Security Card with PGP for Secure E-mail

Hyung-Woo Lee†

ABSTRACT

E-mail system is considered as a most important communication media, which can be used to transmit personal information by internet. But e-mail attack also has been increased by spoofing e-mail sender address. Therefore, this work proposes sender verification faculty for spam mail protection at sender's MTA by using security card for protection forged sender and also for authenticating legal sender. Sender's mail MTA requests security card's code number to sender. Then sender input code number and generate session key after sender verification. Session key is used to encrypt sender's signature and secure message transmission. This work can provide efficient and secure e-mail sender authentication with sender verification and message encryption.

Keywords : Spam-mail, Security Card, Sender Authentication, PGP

1. 서 론

오늘날 컴퓨터와 인터넷의 발달 및 전자상거래의 확산은 우리에게 이메일 사용의 보편화를 가져다주었다. 웹을 통한 메일 시스템인 경우 1인 1 ID를 가지고 있을 정도로 국내 메일 시스템의 활용도는 매우 높다. 그러나 이메일은 불법음란정보의 전달을 손쉽게 하고, 원하지 않는 광고의 계속적

† 정 회 원: 한신대학교 컴퓨터정보소프트웨어학부 교수(교신저자)
논문접수: 2007년 3월 6일, 심사완료: 2007년 3월 29일
* 본 논문은 2007년도 한신대학교 학술연구비 지원에 의해 수행되었음

전달을 가능케 하며, 사이버범죄들을 가능케 하는 등 각종 역기능을 가지고 있다. 이와 같이 폭증하는 스팸 메일로 인해 기업과 사회가 치르는 사회적/경제적 비용도 엄청나게 증가하고 있는 추세이다. 이에 대한 해결 방안으로 기존에 사용하던 스팸방지 시스템은 Filtering, SPF(Sender Policy Framework), RBL(Real-time Blocking List)방식, C/R(Challenge/Response)Filtering 등이 있다. 그러나 이러한 시스템들은 단순한 원칙 및 List에 의한 비교를 통해 스팸 메일을 차단하고 있어 지능화되는 스팸메일에 대한 차단이 어렵다. 그러므로 기존 스팸 메일 방지 기법의 취약점을 해결하기 위해서는 송신자 메일에 자신의 서명을 넣어 송신자에 대한 인증 기능을 제공하고 메일 메시지에 대한 암호화를 통해 기밀성 및 안전성을 제공하는 방법이 필요하다.

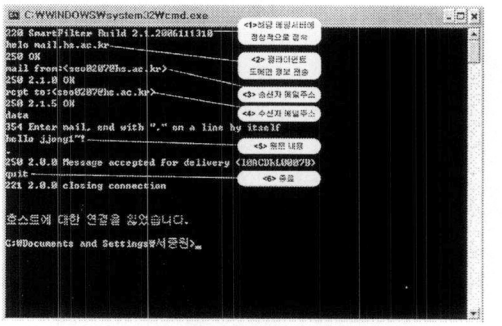
이에 본 연구에서는 스팸 메일에 대한 발신 단계에서 스팸과 관련된 송신 과정을 차단하는 기능을 제공하기 위해 안전성과 보편성 모두를 충족시키고 있는 보안카드를 이용해 DomainKey방식의 메일 발신자에 확인 및 검증 기능을 제공하고 메시지에 대한 무결성 및 안전성을 보장하는 기법을 제안한다. 이 기법은 수신자 측면에서 송신자에 대한 인증 기능을 제공하는 기법이다.

본 논문의 구성은 다음과 같다. I장 서론은 스팸 메일의 현황과 본 연구의 필요성에 대해 설명하고, II장 관련연구 에서는 기존의 스팸 차단 기술과 그 기술의 취약점을 설명하고 보안카드에 대해 설명한다. III장 DimainKey 기법 분석 에서는 DimainKey의 특성 및 인증 기법의 취약점에 대해 살펴본다. IV제안 모델 에서는 제안하는 모델에 대한 설명 및 특징, 필요성과 제안 시스템으로 인한 스팸 차단 효과에 대해 설명한다. V장은 기존 시스템과의 비교분석을 통해 제안 시스템의 특징을 설명한다. VI장 결론에서는 연구 결과의 정리와 향후 연구 과제에 대해 설명한다.

2. 관련연구

2.1 스팸 메일

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 의미한다[1]. 이러한 스팸 메일 발생 원인은 SMTP[2] 기반 메일 송수신 구조를 통해 알아볼 수 있다. SMTP는 인터넷에서 이메일을 보내고 받기 위해 이용되는 프로토콜로 TCP 포트 번호는 25을 사용한다. 현재의 SMTP 기반 메일 전송 시나리오는 <그림 1>과 같다.



<그림 1> SMTP 시나리오

이 과정에서 크게 아래와 같은 이유로 인해 스팸 메일이 발생하게 된다.

- <2>에서 실제 발신 메일 서버 도메인 정보를 속여 전송할 수 있다.
- <3>에서 임의의 발신자에 의해 손쉽게 메일을 송신한다.
- <4>에서 rcpt to 명령으로 다수의 수신자에게 메일을 전송 할 수 있다.
- <5>에서 수신자가 원하지 않는 메일을 메시지를 작성해 전송한다. 이러한 스팸 형식을 막기 위해 원문 내용의 특정 단어에 대한 Filtering 기법이 제안 되었다.

이러한 스팸 메일 발생 원인을 막기 위해 현재 많은 시스템들이 제안 되어 부분적인 효과를 얻고는 있지만 근본적인 방지책인 <3> 임의의 발신자에 의한 메일 송신에 대한 완벽한 대비책이 없는 실정이다. 그럼 기존의 송신자 인증을 통한 스팸 메일 방지 기법의 특징 및 장단점에 대해 고찰하면 다음과 같다.

2.2 기본 스팸 메일 방지 기법

2.2.1 LMAP(Lightweight MTA Authentication Protocol)

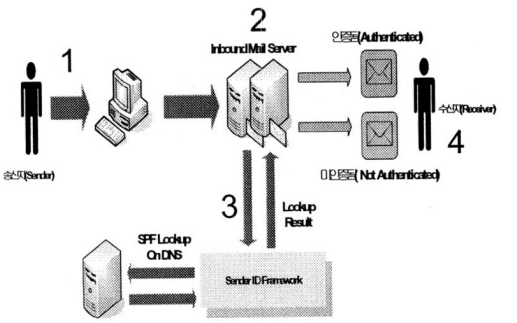
Lightweight MTA Authentication Protocol(LMAP)은 EHLO/HELO에 있는 이름과 MAIL FROM 필드를 이용할 수 있는 SMTP 클라이언트들을 사용하기 위하여 허가된 도메인들에 의해 스팸 문제로부터 주소들을 돕기 위한 제안된 프로토콜들의 집합이다. SMTP 서버들은 클라이언트가 합의 하에 도메인의 이름을 사용하고 있다면 이를 결정하기 위해 이 정보를 이용할 수 있다. 그리고 LMAP는 RMX, SPF, DRIP, MTAMARK 및 FSV를 모두 포함한다.

SMTP 메일 서비스에 있어서 스패머들이 익명의 불법적인 접근이 가장 큰 문제이다. 그래서 LMAP는 송신자에 의해 제공된 발송인의 기계 IP 주소와 SMTP 봉투 도메인들 사이에 관계로서 설치된 제공되는 기능의 지침들에 의해 SMTP를 보강시킬 수 있다.

하지만 기존의 LMAP 프로토콜인 경우 IP Spoofing 기반의 메일 발송 기술에는 취약하다는 단점이 있어 이에 대한 대응 기술이 제시되어야 한다. 또한 하위 레벨에서의 인증 기술만을 제시하여 메일 발신 시스템과 같은 상위 계층에서의 보안 구조가 제시되어야 한다.

2.2.2 Sender ID

<그림 2>와 같이 'Sender-ID'는 모든 이메일 메시지가 나타내는 도메인으로부터 발송되었다는 것을 검증한다. 이것은 그 도메인 소유자나 이메일 수신자가 이메일을 보내는 것을 허락한 서버에 등록된 리스트에 대항해 메일을 보내는 서버의 주소를 검사하는 방식으로 운영된다. 이 검사는 이메일 메시지가 전달되기 전에 인터넷 서비스 제공 사업자(ISP, Internet Service Provider)나 수신자의 메일 서버에 의해 자동적으로 수행된다. 그리고 'Sender-ID' 인증이 되면 그 메시지는 정상적인 메일로서 수신자에게 전달된다. 만약 이 검사에 실패하면 그 메시지는 심층 분석되거나 수신 서버에 의해 차단되거나 사용자가 스팸 메일로 오인할 가능성이 발생할 수 있다.



<그림 2> 'Sender-ID'의 흐름도

2.3 기본 스팸 방지 시스템의 취약점 및 해결방법

송신자 인증방식(Sender-ID)의 스팸메일 차단 기술에 대한 기술적 검증과정이 필요하다. 관련 업계에 따르면, ASTA가 제시한 가이드라인에는 인터넷프로토콜(IP) 주소를 통한 이메일 발신자나 디지털 콘텐츠 서명 등을 기술적으로 검색하는 방법들이 포함돼 있다. MS와 AOL의 경우 ISP 비교 인증 방식을 채택하고 있다. MS는 '이메일 발신자 확인(Caller ID for E-mail)'을, AOL은 'SPF(Sender Policy Framework)' 기술을 각각 개발하고 있는데, 이는 메일에 표시된 주소와 실제 전송된 경로의 IP주소를 비교하여 일치하지 않으면 스팸메일로 간주해 차단하는 방식이다.

근본적인 측면에서 고찰해 본다면 기존 SMTP 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. 따라서 본 논문에서는 보안카드를 송신자 인증 수단으로 사용해 메일 송신자 인증 기법을 제안한다.

2.4 소프트웨어 형태의 보안카드

보안카드는 사용자 인증절차의 보안성을 위해 지정된 사용자에게 발급하는 코드표이다. 고유한 카드번호에 30~35개의 4자리 10진수 코드가 구성되어있으며, 현재 금융, 게임 업계뿐 아니라 다양한 사이버 공간의 인증절차에서 사용되고 있다. 지난 4월부터 국내 금융기관에서는 조합형 입력체계를 사용하여 보안 카드의 보안성을 더욱 높였다. 보안카드의 경우의 수는 다음과 같다.

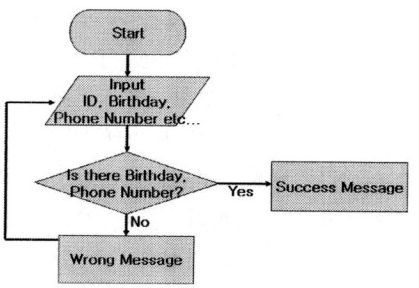
각각의 자리수(4자리)에 사용할 수 있는 숫자는 10개 그러므로 경우의 수는 10,000개이다 이때 카드를 구성하는 코드의 개수가 30~35이므로 카드를 만들 수 있는 조합은 다음과 같다.

$$p(n,r) = n(n-1)(n-2).....(n-r+1)$$

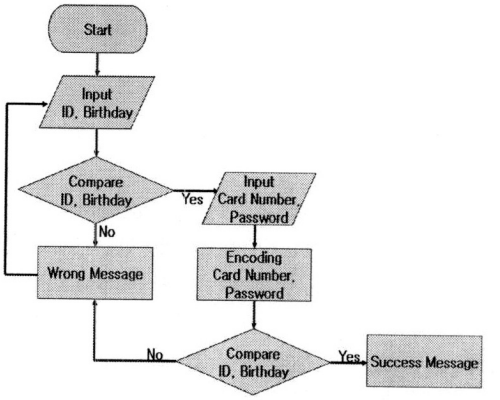
$$p(n,r) = \frac{n!}{(n-r)!} = 9.5739154*10119$$

4자리 숫자 중 35개의 코드를 하나의 보안카드에 만들 수 있고 두 개의 번호를 사용한다면, 10,000*30*29=11,900,000의 경우수를 제공하여 11,900,000개의 One-Time Key를 생산할 수 있다. 본 연구에서는 보안카드의 보안성과 특정 사용자만 사용하는 유일성 그리고 인증 요청 때마다 변하는 가변성의 특징을 이용해 스팸메일 방지를 위한 DomainKey 방식의 송신자 인증 프로토콜에 사용한다.

스팸메일에 대한 인증을 위해 사용되는 소프트웨어 형태의 보안카드를 생성/발급하는 과정은 다음과 같다.



<그림 3> SW 보안카드 생성 초기 단계



<그림 4> 보안카드 생성/검증 단계

위 <그림 3>에서와 같이 SW 형태의 보안카드를 발급하기 위한 초기 설정 과정을 수행한다. 보안카드가 생성되면 사용자는 자신만이 소유한 비밀 정보를 통해 보안카드에 대한 접근 권한을 갖게 되고, <그림 4>와 같이 해당 보안카드 번호를 이용하여 메일 전송 과정에 입력하게 된다. 이와 같은 보안카드 시스템을 메일 전송 과정에 적용하여 보다 안전하면서도 메일 발신자에 대한 이중 인증 기능을 제공할 수 있게 된다. 메일 전송 과정에서 사용되는 기법에 대해 분석하면 다음과 같다.

3. DomainKey/PGP 기법 분석

3.1 DomainKey 전송서버 작동방식

'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 [5].

도메인 키를 통해 메일을 인증하는 데에는 두 가지 단계가 있습니다.

준비 단계 : 도메인 소유자는 발신되는 모든 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.

3.2 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.

3.3 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 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 보안카드를 통한 새로운 발신자 인증 기법을 개발하였다.

3.4 기존 PGP 기법의 특징

기존의 PGP(Pretty Good Privacy)[6] 기반 전자우편 보안 프로토콜에서 사용하는 주요 기법은 다음과 같다.

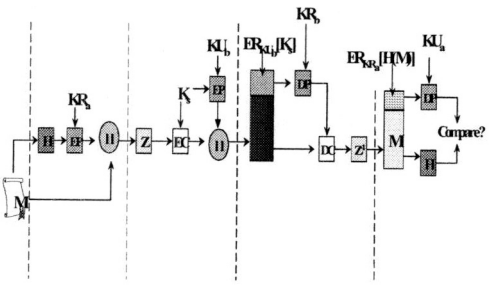
- 디지털 서명
  - SHA-1[8]을 사용하여 해쉬코드 생성
  - DSS 또는 RSA를 사용하여 메시지 다이제스트에 대한 서명
- 메시지 암호화
  - CAST, IDEA[9], 3DES[10], D-H, RSA 사용
- 압축 및 호환성 제공
  - 전장 및 전송을 위해 ZIP으로 압축
  - 암호화된 메시지를 Base-64 코드 적용 후에 ASCII 문자열로 변환

PGP 기법인 경우 Private Key 및 Public Key에 대해서는 Key Ring 개념을 적용하여 사용자

가 사용할 수 있도록 한다. 사용자가 소유한 키 쌍과 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 과정을 아래 <그림 5>와 같다.



<그림 5> PGP 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.

4. 제안기법

본 논문에서는 기존의 스팸 방지 시스템의 취약점을 보완하기 위하여 보안카드를 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

4.1 제안 기법의 특징

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

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 방식과 유사한 키 링 구조를 유지/관리하여야 한다는 문제점이 있다.

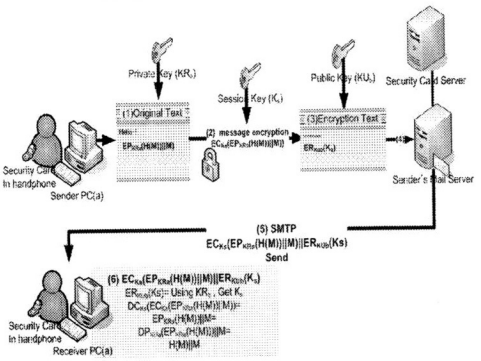
따라서 본 연구에서는 소프트웨어 형태의 보안카드를 개발하여 이중 인증(dual authentication) 기능을 제공하고자 한다. 핸드폰내 보안카드 개념을 적용하여 핸드폰이 갖고 있는 개인 확인 기능을 통해 DomainKey 및 PGP 기반 메일 암호/인증에서 사용되는 비밀 정보를 송신하는 구조를 적용하여 좀더 효율적이면서도 강화된 인증 구조를 제시하고자 하였다.

4.2 제안 모델

기존의 스팸방지 시스템은 송신자 IP, 그리고 필터링 기법들을 이용해 이루어 졌다. 그러나 이런 방식들은 2장에서 설명했듯이 많은 문제점을 가지고 있다. 가장 큰 문제는 송신자의 인증 과정이 없다는 것이다.

핸드폰에 소프트웨어 형태의 보안카드를 이용

한 송신자 인증기법은 특정 송신자에게 유일하게 발급되는 보안카드를 이용해 스팸 메일을 차단할 수 있다는 것에 중점을 맞추고 있다.



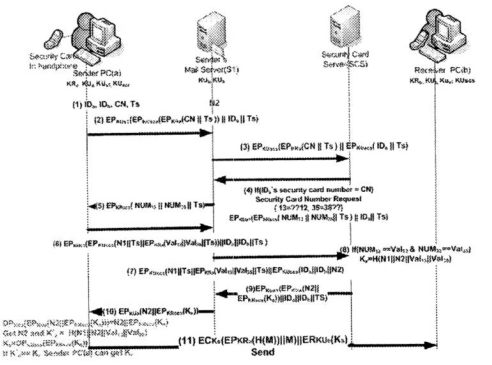
<그림 6> 핸드폰에 탑재된 보안카드를 이용한 제안 시스템 구성도

<그림 6>은 본 논문에서 제시하는 기법에 대한 전체적인 구성도이다. 송신자는 메일을 송신하기 위해 다양한 응용프로그램(POP3, IMAP4, WebMail)에 접속을 한다. 그리고 보안 카드에 의한 Key분배 이후의 과정은 다음과 같다.

- 1단계 : 송신자가 메일을 송신하기 위해 응용프로그램에 접속한다. 메일을 보내기 위해 자신의 개인키를 이용해 메일에 서명을 한다. EPKRa(H(M))||M)
- 2단계 : 송신자의 메일 메시지는 보안 카드에 의해 분배 받은 SessionKey(Ks)를 이용해 송신자의 서명을 암호화 한다. ECKs(EPKRa(H(M))||M))
- 3단계 : 2단계에서 송신자의 서명을 암호화하기 위해 사용한 SessionKey(Ks)는 수신자의 공개키로 암호화해 전송한다. ERKUb(Ks)
- 4단계 : 송신자의 메일 서버로 전송된다. 송신자 메일 서버에서는 전송 메시지에 송신자의 서명이 첨부 되어 있는지 확인한다. 만약 송신자의서명이 이루어 지지 않은 메시지는 스팸 메일로 분류된다.
- 5단계 : SMTP에 의해서 수신자의 메일 서버로 안전하게 전송 된다.
  ECKs(EPKRa(H(M))||M))||ERKUb(Ks)
- 6단계 : 수신자는 수신된 메시지를 복호화 하기 위해 자신의 개인키(ERKab)를 이용해 SessionKey(Ks)를 추출하고, Ks를 이용해 DCKs(ECKs(EPKRa(H(M))||M)))를 복호화 한다. 송신자의 개인키로 서명된 EPKRa(H(M))||M)를 복호화 하기 위해 송신자의 공개키를 이용해 복호화 한다. H(M)||M를 추출한 수신자는 메시지의 내용과 H(M)를 이용해 메시지의 무결성까지 검사 할 수 있다.

4.3 키 생성 및 분배 과정

본 논문에서 제안한 기법은 기존의 송신자 인증과정의 취약점을 보안하기 위해 안전한 공개키/개인키 전송을 위해 SessionKey(Ks)를 사용하였다. SessionKey(Ks)의 효과로는 공개키/개인키의 안전한 전송뿐 아니라 원문 메시지의 암호화까지 수행하므로 보안성이 강화된 스팸 메일 방지 기법이라 할 수 있다. <그림 7>은 SessionKey(Ks)의 안전한 분배를 위해 보안 카드를 이용한 키 생성 및 분배 과정을 보여주고 있다. 또한 강력한 SessionKey(Ks)생성을 위해 조합형 보안 카드를 사용해 보안성을 더욱 높였다.



<그림 7> SessionKey(Ks) 생성 및 분배 과정

본 논문 키 분배 시나리오에서 a는 송신자, b는 수신자를 의미한다. 비밀키 KRx(x=a, b), 공개키 KUx(x=a, b), 공개키 암호화 방식(RSA)[7]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 송신자 및 수신자의 Mail Server에는 모든 ISP업체 및 개인 메일 서버 사용자의 공개키를 가지고 있다고 가정한다. 송신자는 자신의 ID(IDa)와 보안 카드 번호(CN)를 mail server에 전송한다. 그 정보는 다시 Security Card Server(SCS)에 전송되어 가입자의 ID와 보안카드 번호(CN)의 일치 여부를 확인후 Request NUM1, NUM2를 요청한다. 이에 대한 송신자의 Response Val1, Val2와 N1, N2에 의해 키가 생성된다. 구체적인 과정은 아래와 같다.

- 1단계 : 사용자 a는 기본 정보를 생성
  IDa : 송신자에 대한 정보
  IDb : 수신자에 대한 정보
  CN : 보안카드의 고유 번호
  TS : 사용시간에 대한 정보
- 2단계 : 송신자 a는 request number 요청
  EPKUs1(EPKUscs(EPKRa(CN||TS))||IDa||TS)
  - 송신자는 자신의 개인키를 이용해 보안 카드 번호(CN), 키 사용 시간(TS)에 대한 정보를 서명한다.
  - EPKRa(CN||TS)은 Security Card Sever의 공개키로 암호화된다.
  - EPKUscs(EPKRa(CN||TS))은 송신자의 사용자 정보(IDa)와 키 사용 시간(TS)와 연접해 메일 서버(S1)의 공개키로 암호화된다.
- 3단계 : 메일 서버(S1)은 Security Card Server(이하 SCS)에게 Security Card Number Request를 요청
  - EPKUscs(EPKRa(CN||TS))은 Security Card Server 만이 복호화 할 수 있다.
  - EPKUscs(IDa||TS)을 이용해 사용자(IDa)의 CN과 전송 받은 CN의 일치 여부를 확인 할 수 있다. 만약 불일치 시 Security Card Number Request는 취소된다.
- 4단계 : SCS는 조합형의 보안카드로 임의의 코드 번호 2개의 각각2자리씩 송신자에게 요청한다. 예로[그림6]에서는 13의 뒷자리 2개, 35의 앞자리 2개를 들었다.
  - EPKRscs(NUM13||NUM35||TS)은 보안카드 서버의 개인 키를 이용하여 서명하고, 송신자는 보안카드 서버의 공개키를 이용하여 검증한다.
  - EPKUs1(EPKRscs(NUM13||NUM35||TS)||IDa||TS)은 송신자 정보(IDa)를 연접하여 메일 서버의 공개키로 암호화하여 전송된다.
- 5단계 : 송신자 Request Number 수신
  - 송신자는 메일 서버로부터 안전하게 Request Number를 전송 받는다.
- 6단계 : Request Number에 대한 Response
  - 송신자는 자신의 서명이 들어간 EPKRa(Val13||Val13||TS)를 이용해 Request Number에 대한 Response를 전송한다.
  - 이때 Session Key(Ks)를 생성하기 위한 임의의 난수 N1값은 TS와 연접해 SCS의 공개키로 암호화된다.

  EPKUscs(N1||TS||EPKRa(Val13||Val13||TS))
  - 메일 서버에게 송수신자의 정보(IDa, IDb)와 TS를 연접해 메일서버의 공개키로 암화화해 전송해 준다.

  EPKUs1(EPKUscs(N1||TS||EPKRa(Val13||Val35||TS))||IDa||IDb||TS)
- 7단계 : SCS에게 Response 전달
  - 메일 서버(S1)은 송신자로부터 전달 받은 Response(Val13, Val35)를 SCS에게 전달한다.

  EPKUscs(N1||TS||EPKRa(Val13||Val13||TS)
  - EPKUa(IDa||IDb||N2)를 전송해 이 Response의 송신자 및 송신자가 메일을 전송하려는 수신자의 정보, Session Key(S1)생성을 위한 임의의 난수 N2를 SCS의 공개키를 이용해 전달한다.
- 8단계 : 송신자 인증 및 키 생성
  - SCS의 요청으로 전송된 Val13과 Val35가 정확한 값인지 확인 절차 후 일치된 값일 경우 송신자에 대한 인증 및 키를 생성한다.
  - 이때 Session Key(Ks)는 송신자에 의해 생성된 N1, 메일서버에 의해 생성된 N2 그리고 Val13, Val35의 해쉬 함수로 생성된다.
- 9단계 : Session Key 전송
  - EPKUs1(EPKUa(N2||EPKRscs(Ks))||IDa||IDb||TS)를 SCS 로부터 전송 받은 메일 서버는 송신자의 정보와 Key의 사용시간 정보(TS)를 인지한다.
- 10단계 : Session Key 전송 및 검증
  - EPKUa(N2||EPKRscs(Ks))를 전송 받은 송신자는 DPKRa를 이용해 N2를 얻는다. 그리고 SCS의 공개키를 이용해 Ks를 얻는다.
  - 송신자의 메일 응용 프로그램들은 N1(송신자가 생성한 값), N2, Val13, Val35를 해쉬한다.
  - 해쉬된 값이 Ks와 같을 때 Session Key(Ks)이 대한 무결성을 보장하고 송신자는 Ks를 이용해 메시지를 암호화 한다.
- 11단계 : Ks를 이용한 메시지 전송

<표 1> 기존 기법과의 안전성 및 성능 비교 평가

특성 / 기법	스팸차단방식	발신자 인증기능	메일 암호화	무결성 제공	안전성	보안카드 접목기능	비고
Filtering 기법	메일내용필터링	×	×	×	×	×	메일컨텐츠필터링방식
SPF	IP주소기반	△	×	×	▽	×	DNS검색방식
DomainKey	발신자인증	△	◇	◇	◇	×	공개키암호화방식
PGP	해당사항 없음	◇	△	△	△	×	키링방식
제안한 기법	발신자 인증	△	△	△	△	○	이중인증

○: A ×: N/A △:good ◇:moderate ▽:bad

- ECKs(EPKRa(H(M)||M))||ERKUb(Ks)를 수신자 b에게 전송한다. 이때 Session Key(Ks)는 b의 공개키로 암호화된다.
- 송신자의 서명이 첨부된 원문 메시지 EPKRa(H(M)||M)는 Ks를 이용해 함호화 된다.

4.4 송신자 인증 및 암복호화 과정

본 논문에서 송신자는 자신이 보내려는 수신자의 공개키를 얻을 수 있으며 자신의 개인 키는 이미 안전한 곳에 저장되어 있다. 그리고 Ks는 보안카드의 코드 번호로부터 생성할 수 있다. 이때 보안 카드의 One-Time Key를 이용하므로 패킷 스니핑 등의 공격에 안전하다고 할 수 있다. 원문 메시지의 EPKRa(H(M)||M)를 통해 메시지의 무결성을 보장하고 있다. 이 값은 메시지 암호화를 위해 관용암호방식을 이용해 Ks를 세션키 값으로 이용해 메시지를 암호화 한다. 그러나 수신자는 Ks를 모르므로 수신자의 공개키(KUb)를 이용해 Ks를 암호화 한다. 최종적으로 전달되는 메시지는 ECKs(EPKRa(H(M)||M))||ERKUb(Ks)이다.

수신자는 자신의 개인키와 송신자의 공개키를 알고 있다. 우선 자신의 개인키를 이용해 Ks를 추출한다. DCKs(ECKs(EPKRa(H(M)||M)))를 해 EPKRa(H(M)||M)를 추출한다. 그렇게 나온 H(M) 과 연접했던 M를 해쉬한 H'(M)과 비교해 송신자의 메시지 무결성을 검증한다. 위와 같은 과정은 기존의 DomainKey 및 PGP 방식과 유사한 과정을 수행하게 된다.

5. 안전성 평가 및 비교 분석

5.1 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 보안카드가 갖고 있는 One-Time Key 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 장

점이 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.

5.2 제안 기법의 안전성 평가

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

6. 결 론

본 연구에서 제안한 모델은 11,900,000개의 One-Time Key를 제공하는 보안 카드 방식을 이용하고, 핸드폰 기반의 개인인증 방식을 적용하여 e-mail 메시지에 대한 암복호화 및 송신자 이중 인증 모델을 제안하였다. 보안 카드는 온라인 개인 인증 과정에서 사용량이 날로 높아져가고 있는 기법으로 안전성과 보안성은 이미 검증 받은 상태이다. 단순한 필터링 기법 또는 스팸 송신자 리스트 비교 방식 등을 통한 기존의 스팸 차단 기법과 달리 본 연구에서 개발한 기법은 소프트웨어 형태의 보안 카드를 이용하여 메일 송신자에 대한 인증을 수행하는 방식으로 근본적인 스팸 차단 기능을 제공한다.

앞으로 개인인증과 개인정보보호 분야에 많은 관심과 기술이 집중될 전망이다, 그러므로 본 논문에서 제안한 이중 발신자 인증 체계를 접목한다면 보다 다양하고 안전한 스팸 차단 방식으로 발전시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] 이종희, 범람하는 스팸 메일과 대응현황, http://seri.org/db/dbThemV.html?menu=db0901&tgbn=05&menu_gbn=070100000&pub_key=wb20000902375

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

[3] Pam Cocca, "Email Security Threats", SANS Institute 2005, September 20, 2004.

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

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

[6] Jay D. Dyson, "Public Key Cryptography & PGP" 1999.

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

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

[9] 이임영, 송유진, "현대 암호화", 생능출판사, 1999.

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

이 형 우

1994 고려대학교 컴퓨터학과 (이학사)
1996 고려대학교 컴퓨터학과 (전산학 석사)
1999 고려대학교 컴퓨터학과 (전산학 박사)
1999~2003 천안대학교 정보통신학부 교수
2003~현재 한신대학교 컴퓨터정보소프트웨어학부 부교수
관심분야: 정보보호, 네트워크보안, 무선보안
E-Mail: hwlee@hs.ac.kr