차세대 이메일 보안 기술에 관한 연구*

김 귀 남**

요 약

이메일은 언제 어디서나 실시간으로 전송될 수 있는 이점으로 인하여 그 역할이 증대되어 왔다. 하지만, 오늘날 이메일 보안 위협은 점차 지능적으로 특정 기관에 대한 공격으로 변화되고 있다. 이러한 상황에서 위협 대응에는 많은 한계가 있다. 따라서 이메일의 개념을 파악하고, 나날이 변화하는 정보기술 환경 변화속에서 발전되는 차세대 이메일 서비스 체계를 정립하고자 한다. 이를 토대로 이메일 환경에 대한 악의적 공격기술인 악성코드, 사회공학기법을 이용한 해킹 공격, 하이브리드 웜, 바이러스, 중요 메시지 갈취, 비인가된 계정 접근 등에 대한 정보를 수집하여, 공격 양상 변화 과정 파악 및 분류 체계를 정립하고 향후 변화 방향을 분석한다.

A Study on the Security Structure of Next Generation E-mail System

Kuinam J. Kim**

ABSTRACT

E-mail's role has been increased due to its merit which is sending demanded information in real-time anywhere, anytime. However, Today's E-mail security threats have being changed intelligently to attack against the specific agency. The threat is a limit to respond. Therefore precise definition and development of security technology is needed to analyze changing environment and technologies of e-mail so that remove fundamental security threat.we proposed Next Generation E-mail System Security Structure and the Next Generation fusion System using authentication As a result, in this study, we development of Next Generation E-mail System Security Structure. This system can protect E-mail user from social engineering hacking technique, spam, virus, malicious code and fabrication.

Key words : Email, Security, Fusion System

* 본 연구는 2007학년도 교내연구비 지원에 의해 수행되었음.
** 경기대학교 정보보호학과

1. 서 론

현대 사회는 정보통신기술과 인터넷의 발달로 인해 엄청난 부가가치를 창출하고 있으며, 정보통신 시스템 및 네트워크는 다양한 기반 기술 개발과 고급 응용 기술의 융합으로 인해 더욱 다양화되고 있다. 이러한 흐름 속에서, 비즈니스 영역 또는 개인의 필요에 따른 전자적 메시지 교환을 가능하게 하는 이메일 관련 기술도 함께 발전되어 왔다. 이는 중요 메시지의 송신자와 수신자 사이의 시간적·공간적 제약을 해소하였고, 언제 어디서나 필요로 하는 곳으로 요구된 정보를 실시간으로 전달할 수 있다는 장점으로 인하여 그 역할이 증대되어 왔다.

그러나 정보 사회의 발전 양상 속에서는 해킹, 바이러스, 정보유출, 변조, 파괴 등의 보안 사고들도 함께 증가하고 있다. 이러한 정보화 순기능과 역기능의 동시적 발전은 전자적 시스템을 이용한 정보 교환 분야에서도 동일하게 나타나고 있다. 특히 현대 정보화 사회에서 사용되고 있는 이메일은 그 이용도와 중요도가 급격히 증가하고 있지만, 만연되어 있는 보안 불감증과 기술적 취약점으로 인해 사용자들에게 큰 피해를 입히고 있다. 따라서 변화하는 이메일 사용 환경 및 기술 요소들을 분석하고 이를 통해 원천적인 이메일 보안 위협 요소를 제거할 수 있는 보안 기술의 명확한 정의 및 개발이 요구된다. 본 연구에서는 이러한 문제점을 인식하고 실질적인 위협원 식별, 관련된 보안 기술 정의, 기능 명세 및 요구를 통하여 차세대 이메일 보안을 위한 융합시스템 구조를 수립하도록 한다.

2. 관련연구

2.1 Active Contents 공격

메일을 열람할 경우 HTML 기능이 있는 이메일 클라이언트나 웹브라우저를 사용하는 이용자를 대상으로 하는 공격 기법이다. 메일을 열면 자바스크립트나 비주얼 베이직 스크립트가 자동으로 번역되는 취약점을 이용하여 스크립트 내부에 악성 실행코드를 삽입하여 피해자의 컴퓨터에서 정보를 유출하거나 피해를 입히는 방법이다. 그 예로는 수신자가 메일을 열어볼 때 음란 사이트나 광고 사이트를 보여주도록 하거나 시스템을 마비시키는 서비스거부공격(Denial of Service)을 시도하는 방법이다.

(사례) VBS(Visual Basic Script) 웜 바이러스

2.2 Buffer Overflow 공격

MIME의 헤더를 변경하여 헤더의 길이가 메모리상의 버퍼 크기보다 클 경우 헤더의 내용이 데이터 부분을 덮어쓰는 단점을 이용하여 헤더 내부에 악성 실행코드를 삽입하는 공격 기법이다. 실제로 CERT(Computer Emergency Response Team)에서 MS Outlook과 Outlook Express의 버퍼오버플로우 취약점을 공지한 경우가 있다.

(사례) Nimda 웜바이러스

2.3 Trojan Horses 공격

이메일을 통하여 악성실행파일을 유포하고, 수신자로 하여금 첨부된 파일을 실행하도록 권유하여 Trojan 프로그램을 실행하게 하는 공격 방법이다.

(사례) loveletter 바이러스, annakornikova 바이러스

2.4 Shell Script 공격

특정 메일 프로그램이 메일 메시지에 내장된 쉘 명령을 지원하는데, 이를 이용하여 메일 헤더를 조작하여 해당 시스템에서 특정 명령이 수행되도록 하는 공격 기법이다.

2.5 Bombing과 Spamming

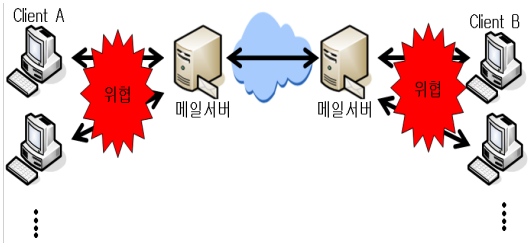
발신자의 정체를 숨기고 특정 주소로 같은 메일을 계속 보내는 Bombing과 Bombing의 변종으로 수백~수천의 불특정 다수에게 메일을 전송하는 Spamming 공격 형태는 아직까지 뚜렷한 대응 방안이 없는 실정이다. 이러한 공격을 받을 경우 네트워크 과부하를 초래하고 메일 서버의 경우 시스템 자원의 소모 및 하드디스크 고갈을 초래할 수 있는 치명적인 방법이다[3-5].

3. 차세대 이메일 보안 위협 분석

차세대 이메일 시스템을 위한 보안 구조는 현존하는 이메일 시스템의 보안 기능을 더욱 강화시키며, 새로이 나타나고 있는 서비스의 개인화 및 기술의 컨버전스 환경에서도 적용될 수 있도록 개발되어야 한다. 이는 이메일 시스템과 관련된 정보기술 환경이 가지고 있는 보안 위협은 지금도 그대로 존재하고 있기 때문이며, 더욱 지능적이고 다양하게 변화하며 나타나고 있기 때문이다. 또한 기존에 발생하고 있는 사이버 위협들을 해결하지 못한다면, 새로운 보안 기술의 적용도 어렵기 때문이다. 따라서 본 장에서는 발전하는 이메일 환경에서 적용 가능한 보안 기술을 예측하여 이를 토대로 차세대 이메일 시스템이 가지는 유형별 위협에 관하여 살펴보기로 한다.

3.1 클라이언트/서버 간 보안 위협

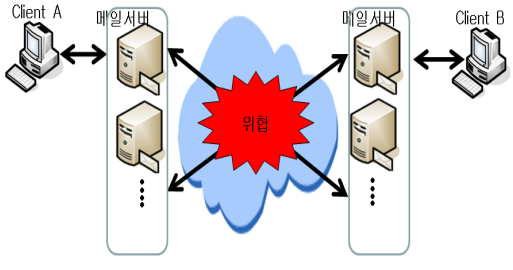
(그림 2)에서 나타난 것처럼 송신자와 메일서버, 수신자와 메일서버 사이에서 보안 위협이 발생할 수 있다. 공격자는 송신자 A와 메일서버 사이에 위치하여 전송중인 메일을 스니핑 하거나 조금 더 지능적인 경우 그 내용을 변조할 수도 있다. 또한, 수신자B의 경우는 수신된 메일로부터 바이러스에 의한 감염이나 피싱 사이트를 소개하는 유해성 메일을 수신할 수도 있다. 중요한 메일의 경우, 스니핑과 메시지 변조를 막기 위해서는 고비용이 들더라도 암호화 기술 등을 사용할 필요가 있다.



(그림 2)클라이언트/서버 간 보안 위협

3.2 메일 서버 간 보안 위협

Client(송신자) A는 (그림 3)과 같은 공격 시스템을 구성하고 대량의 메일을 전송하여 메일 서버를 다운시키거나 스팸메일을 유포할 수 있다. 또한, 전송중인 패킷을 가로채어 그 내용을 변조할 수 있으며, 특정 발신자로 위장하여 메일을 전송할 수도 있다. 이러한 보안 문제를 해결하기 위해서는 수신 메일서버의 인증기능을 강화해야 한다. 즉, 합법적인 송신서버로부터 메일이 전송되었는지 확인하는 기능이 제공되어야 한다. 또한, 수신 메일서버 앞단에 필터링 게이트웨이를 설치하여 스팸메일을 차단하거나 대량 메일이 전송되는 조기 징후를 파악할 수 있는 시스템 구축도 필요하다.



(그림 3) Firewall에서 나오는 로그 형태

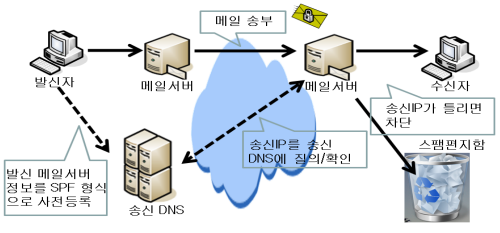
4. 차세대 이메일 보안 구조

차세대 이메일 보안 기술은 이메일 서비스의 신뢰성을 보장하여 안전한 전자 메시지 전송 체계를 구현하기 위해 추진된다. 이는 이메일 시스템에서 작성, 저장 및 유통(송/수신)되는 정보의 기밀성(정보 누출 방지)과 무결성(데이터 위·변조 방지)을 보장하며, 이메일 시스템의 안전성과 가용성을 향상시키는데 필요한 핵심 기술들을 총칭한다. 세부적으로는 인증기술, 암호기술, 스팸 차단 기술, 필터링 기술, 이상 징후 조기탐지 기술 등을 유기적으로 연계하고 융합하는 시스템으로 생각할 수 있다.

4.1 인증기술

SPF를 사용하는 도메인은 반드시 적법한 SPF Record를 발행하여야 하며 발송하지 않은 도메인은 SPF Recording을 위해 ID, Domain, Sender 등과 같은 SPF 발신자 정보를 SPF Record에 포함하여 인증을 받아야 한다.

SPF는 이메일주소와 발송 IP가 다른 이메일을 완벽하게 구분해서 이메일헤더에 표시해주기 때문에 어떤 이메일서버에서도 이메일헤더를 필터링하면 스팸메일로부터 안전하다는 장점이 있다. (그림 4)은 SPF의 동작 과정을 보여준다.



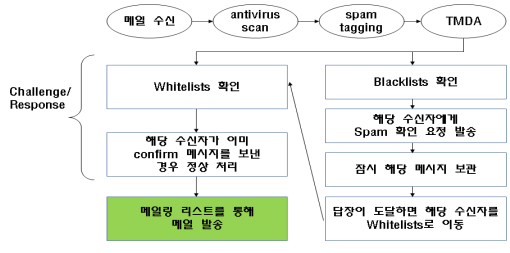
(그림 4) SPF의 동작 과정

4.2 스팸차단기술

차세대 이메일 시스템은 스팸 및 악성코드를 필수적으로 차단할 수 있어야 한다. 대부분의 공개 서비스 중, SMTP 서비스를 운영하는 것은 그 자체가 위험성을 가지고 있다는 점을 주의해야 한다. 메일 서버에서 어떤 특정한 코드를 실행하여 서버로 침입(exploit)할 수 있는 가능성이 존재하기 때문이다. 이메일 서버를 운영함에 있어서 이메일 시스템을 보안안전지대(DMZ)에서 운영 및 방화벽(Firewall) 바깥에 이메일 시스템을 설치함으로써 악의를 가진 사용자가 침입했다 하더라도 내부의 주요 네트워크 시스템까지는 들어오지 못하도록 하여야 한다. 또한 이메일 서버는 수시로 서버 프로그램을 업데이트해야 하며 버그를 통한 침입을 막기 위한 보안관련 패치를 주기적으로 실행해주어야 한다. 또한 엄격한 보안 정책의 수립으로 잠재적 위험이 있는 첨부파일의 제거를 통해 서버로 침투하는 악의적은 코드의 위험을 줄여야 한다.

4.2.1 TMDA(Tagged Message Delivery Agent)

스팸 및 악성코드 차단을 위해 그룹 형태의 TMDA와 오픈 형태의 DKIM을 기반 구조로 설계되는 것이 타당하다. TMDA는 현재 이메일 시스템에 등록된 모든 사용자를 화이트 리스트(Whitelists)에 포함하고 주요 스팸 송신자에 대해 블랙리스트(Blacklists)에 포함된다. 새로운 사용자는 화이트 리스트에 포함되기 위해 확인 메일이 전달되며 이를 통해 화이트 리스트에 포함될 수 있도록 한다. (그림 5)는 TMDA 시스템의 동작과정을 보여준다.



(그림 5) TMDA 시스템 동작 과정

4.2.2 Real-Time Block List

Real-Time Block List(RBL) 방식은 릴레이가 허용된 시스템이나 스팸을 보내는 것으로 확인된 메일서버의 주소를 데이터 베이스화 한 후, 수신측 메일서버가 해당 메일 서버로부터 발송되어지는 메일의 수신을 거부하는 방식으로 스팸메일을 차단한다. Blocking List는 RBL Operator에 의해 관리되며, 수신측은 Blocking List의 관리에는 관여하지 않는다. 다만 수신측의 메일서버는 송신측으로 Blocking List에 송신서버가 존재한다는 사실을 알려야 한다. 송신측 서버는 RBL Operator와 교섭하여 RBL의 Blocking List에서 자신의 메일서버를 삭제할 수 있다.

4.2.3 컨텐츠 필터링 방식

네트워크에 접속하는 인터넷 웹사이트를 지정한 문자를 바탕으로 필터링하여 사전에 스팸메일을 차단

- 컨텐츠 필터링

URL과 키워드 기반의 웹 사이트, 웹페이지의 접근 차단

- 스크립트 필터링

4.2.4 서버필터링

- 접속 단계 서버필터링

메일 서버에 위협 요소를 가하는 IP로부터의 접속을 제한 한다. 시간당 접속 횟수 제한, 일정 시간동안 기준치 이상의 메일을 보내는 IP를 자동으로 탐지하여 지정 시간 동안 해당 IP의 접속을 차단한다.

- 지능형 베이시안 필터링

스팸메일은 주로 선정적인 단어의 사용과 상업사이트임이 확실한 웹 주소 등 특정한 패턴의 문장을 포함하게 된다. 스팸메일을 받을 때마다 베이시안 필터에 메일을 넘겨주면 필터가 이를 분석해서 단어별로 스팸일 확률을 계산한다. 어느 정도의 스팸 단어 데이터베이스가 구축이 되고 나면 상당히 정확한 확률로 스팸 여부를 판별한다.

4.3 이상 징후 조기탐지 기술

(그림 6)의 핵심은 허니팟, 허니넷으로 이는 시스템을 공격하거나 침입하는 해커에 대한 정보를 수집하기 위해 제작된 허위 서버들이나 시스템들이다. 여기서, 허니 시스템이란 해커나 사이버 악성공격에 의해 공격당함으로써 그 가치를 발휘하는 시스템을 의미하는 것으로 공격자의 정보를 수집하고 이를 이용하여 보안 강화에 도움이 될 수 있는 정보를 제공하는 시스템을 의미하는 것이다. (그림 6)은 불용 이메일에 대한 이벤트에 대해서 공격이라고 사전 정의 후 이벤트탐지패턴 검사 및 행위기반탐지를 통해 비 매칭 이벤트와 매칭 이벤트를 구분하고 구분된 정보를 주성분 분석법으로 해석한다.

(그림 6) 이상징후 조기탐지 시스템 흐름도

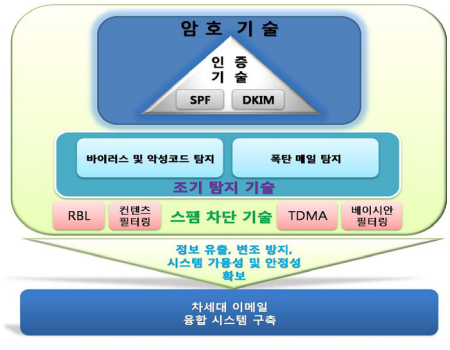
이상 징후 이벤트를 분석하기 위해 PCA(Principal Component Analysis, 주성분 분석)으로 해석이 필요하다. 다차원의 데이터를 거기에 포함된 정보의 손실을 가능한 한 적게 해서 2차원 혹은 3

차원의 데이터로 축약하는 분석방법이다. 주성분 분석을 활용하면 관측 대상이 어떠한 위치에 있는지 시각적으로 파악할 수 있게 해 준다.

4.4 차세대 이메일 시스템 - 융합시스템

4.4.1 융합 시스템 체계

융합 시스템의 궁극의 목표는 이메일 시스템을 통한 정보 유출, 변조를 방지하고 시스템 자체의 가용성과 안정성을 높이는 것이다. 기업의 일급 기밀과 같은 정보의 중요도에 따라 내용 기반 필터링 기술이 요구되며, 필요한 경우 정보 유출과 변조를 방지하기 위해 암호기술이 적용되기도 한다. 암호기술은 그 적용 단계에서 키 분배를 위한 인증기술이 선행으로 요구된다. 기본적인 이메일 사용자의 인증뿐 만이 아니라, 수신 서버에서의 발신 서버 인증 또한 요구된다. 이는 스팸 메일 차단을 위해 요구되는 요소기술이다. 스팸 메일 차단을 위해서는 인증기술 뿐만이 아니라 특정 단어나 URL에 기반한 지능형 베이시안 필터링을 통해 피싱 사이트 그리고 악성코드 등을 검출해 내는 기술도 필요하다. 또한, 대량의 폭탄 메일과 같은 위협으로부터 이메일 시스템을 전반적으로 보호하기 위해 징후를 조기 탐지하는 기술도 요구된다. (그림 7)은 차세대 이메일 시스템의 유기적인 융합 관계도를 나타낸다.



(그림 7) 융합 시스템 체계도

4.4.2 융합 시스템 개발 프로세스

(1) 기관이나 조직의 이메일 시스템 사용 환경 분석

사용자의 이메일 사용 환경을 분석하고 정보에 대한 접근권한을 설정한다. 또한, 사용자의 위치를 고려하여 내부망과 외부망을 분리하고, 기존의 네크워크 보안 장비의 배치를 검토한다.

(2) 인증기술 적용 환경 검토

이메일 사용시에 발생 가능한 정보 유출 및 변조를 방지하기 위한 사용자 인증 기술과 메일 서버 간의 신뢰성을 위한 인증 기술 적용 환경을 검토한다. 적용 환경에 따라 PGP(Pretty Good Privacy), S/MIME(Secure MIME) 또는, SPF(Sender Policy Framework)나 DKIM(DomainKeys Identified Mail) 등의 기술을 선별한다.

(3) 정보 등급에 따른 암호기술 판정

경우에 따라 이메일 시스템을 통해 중요 정보들이 외부로 송신되는 경우가 발생한다. 합법적인 경우 암호기술이 적용되어야 하고, 불법적인 경우는 로깅 및 접근권한 판정 그리고 내용 기반 필터링을 통해 차단해야 한다.

(4) 인증기술 및 필터링 기술을 접목한 스팸 차단 기술 적용

인증기술 만으로는 스팸 차단 기능을 완벽히 구현할 수 없기 때문에 합법적인 이메일 전송자로부터 발생할 수 있는 피싱 사이트 유도성 사용자기만 행위와 원치 않는 대상으로부터의 메일 수신을 차단하기 위한 스팸 차단 기능을 고려해야 한다.

(5) 융합 이메일 보안 시스템 구축 및 디버깅

기 열거한 보안 기술과 기존 네트워크 보안 장비들을 적소에 배치하고, 이메일을 통한 네트워크 상의 이상 징후 시그니처를 탐지할 수 있는 모듈

을 탑재하여 융합 보안 시스템을 구축하고 디버깅을 실시한다.

(6) 지속적인 모니터링 및 엔진 업데이트

모니터링은 사용자의 업무 환경 분석 단계에서부터 시스템 구축에 이르기까지 꾸준히 진행되고, 그 결과를 반영하여 보안 위험성을 점검하고 임계 쓰레숄을 넘을 경우 새로운 적용 가능 시스템을 설계하고 업데이트하도록 한다.

5. 결 론

최근 날로 증가하고 있는 사이버 공간 상의 각종 침해사고로부터 개인 및 기업 정보를 보호하고, ISP 사업자로서 네트워크 시설의 안정적 운용과 시설 자원의 보호를 위해서는 인터넷상의 가장 대중화된 서비스인 이메일에 대한 보안 대책이 필요하다. 현재 대부분의 이메일은 S/MIME나 PGP와 같은 특별한 보안 프로그램을 사용하지 않기 때문에 기밀성, 인증, 무결성이 보장되지 않는다. 만약 S/MIME이나 PGP를 사용하지 않는다면 IPsec과 같은 IP 계층의 보안을 라우터나 방화벽에 적용하여 인증과 데이터 암호화를 통한 이메일의 보안을 보장할 수 있을 것이다. 그러나 라우터나 방화벽을 이용한 IP 계층의 보안을 실행할 경우 라우터나 방화벽 내부의 이메일 보안이 보장되지 않는다. 따라서 어플리케이션 계층에서의 이메일 보안이 필요하다. 차세대 이메일 시스템은 앞서 언급한 여러 가지 다양한 보안 기술들(인증기술, 암호기술, 스팸차단 기술, 이상 징후 조기탐지 기술 등)을 사용자 업무 환경에 따라 유기적으로 연계하는 융합시스템으로, 이메일 시스템의 운영 과정에서 발생할 수 있는 정보의 유출, 변조에 대한 강인성을 제공하고, 이메일 시스템 전반에 걸친 가용성과 안정성을 향상시키는 구조로 진화가 예상된다.

참 고 문 헌

[1] James F. Kubose, Keith W. Ross, “A Top-Down Approach Featuring the Internet.”
[2] William Stallings, “Cryptography and Network Security Principles and Practice.”
[3] Fred Avolio, David Piscitello, “E-mail Security.”
[4] 조유희, 최창효, 박승언, 한세진, “E-mail 보안.”
[5] 이현우, “메일 필티링을 통한 E-mail 보안.”
[6] 정보보호기술 강국도약을 위한 기술개발 5개년 계획수립 워크샵.
[7] Matthew Strebe, “네트워크 보안과 해킹방어.”

김 귀 남
미국 캔자스대학(공학사)
미국 콜로라도주립대학 (공학석사)
미국 콜로라도주립대학 (공학박사)
현재 경기대학교 정보보호학과 교수
현재 경기대학교 산업기술보호특화센터장