제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

SMTP 보안 게이트웨이의 구현

민지영*, 김현구**, 장범환**, 정태명*
*성균관대학교 정보 통신 공학부
**성균관대학교 정보 통신 공학과
e-mail:{zymin, hkkim, bhchang}@rtlab.skkr.ac.kr
tmchung@ece.skku.ac.kr

Implementation of Secured SMTP Gateway

Zee-Young Min*, Hyun-Koo Kim**, Beom-Hwan Chang**,
Tae-Myung Chung*
*School of ICE, Sunhkyunkwan University
**Dept. of ICE, Sungkyunkwan University

요약

인터넷의 확산과 더불어 전자 우편의 사용이 크게 늘면서 스팸메일의 심각성이 대두되고 있다. 현재 스팸메일을 막기 위한 여러 가지 기법이 제안되고 있으나, 대부분의 방법이 메일 서버내의 정책에 따른 메일 필터링으로, 스팸메일로 인해 네트워크 자원이 소실되는 문제는 여전히 해결되지 않고 있다. 또한 여러 메일 서버가 같은 내용의 메일로 반복적으로 공격을 당하게 된다. 본 논문에서는 게이트웨이 수준에서의 메일감시를 통하여 불필요한 스팸메일로부터 네트워크 자원을 보호하고, 내부 메일 서버 전체를 보호 할 수 있는 시스템에 대해 논의 해보고자 한다. 커널 레벨에서의 패킷 감시로 속도가 빠르고, 또한 가상의 커넥션을 맺어 게이트웨이에서 메일을 완전히 받은 후 검사 하므로 더욱더 다양한 정책으로 SMTP를 감시할 수 있으며, 이 시스템은 IP 기반의 다른 프로토콜이나 타 서비스로의 응용 또한 기대할 수 있다.

1. 서론

인터넷이 급속히 확산되고 발전된 지금, 인터넷을 기본으로 하여 중요한 통신수단으로 자리 잡은 전자 우편 서비스는 현재 '스팸메일'이라는 부작용을 겪고 있는 현실이다.

스팸메일이라는 것은 수신을 원하지 않는 사람에게 강제로 전자 우편을 보내는 것을 말하며, 스팸 메일은 최근 몇 년 동안 대두된 심각한 문제이다.

일반적으로 사용자가 인터넷을 이용하기위해 이용료를 지불하는 입장이기 때문에, 스팸 메일의 경우 원하지 않는 메일 때문에 시간을 지체하게 되고 그에 따른 금전적인 손해를 본다는 문제가 있다.(사용자가 모뎀을 사용할 경우에는 돈을 낭비하게 되며, 시간제 서비스가 아닐 경우에도, ISP 업체에서 비용이 들게 된다.) 또한 일반적으로 스팸 메일은 같은 내용의 메일을 많은 사용자에게 무차별 전송하는 행위로써, 네트워크 자원의 소실을 가져온다.

본 논문에서는 게이트웨이에서 스팸메일을 원천적으로 차단하여, 네트워크 내부 자원을 스팸메일에 의한 트래픽으로 보호하고, 네트워크 내부의 메일 서버 전체를 보호할 수 있는 방안에 대해 논의 해보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 스팸메일에 대한 현재 연구 사례와 문제점을 살펴보고, 3장에서 본 시스템인 Secured SMTP Gateway(이하 SSG)의 구조를 설명한다. 4장에서 실제 구현 방식을 보여주고, 5장에서 결론 및 향후 계획에 대해 얘기하겠다.

2. 관련 연구

기존의 스팸메일에 대한 기술적인 대처나 SMTP

관련한 관리에 대한 기술에 대해 알아보았다.

2.1. 데이콤의 특허 신청안

특2002-00011번[1]으로 데이콤이 기술을 고안하여 특허를 신청하였다. 이 기술은 일반적으로 스팸메일을 보내는 사람들은 인터넷 게시판 등에 공개된 메일 주소를 수집하여 주소 리스트를 만들어 사용하는 경우가 많다는 점을 착안한 것이다. 실제 존재하지 않는 이 메일 주소를 인터넷에 유포하여 스팸 메일을 보낼 의도가 있는 자에 의해 수집되게 유도한다. 그리고 본 서버에서는 유포한 존재하지 않는 이 메일 주소가 포함된 메일은 스팸메일로 간주하는 방식을 고안하였다. 이것은 스팸메일을 알아내는 효과적인 방법이다. 하지만, 결국 메일 서버는 스팸메일을 받게 되고, 검사이후 삭제하므로, 이용자는 보호되지만, 네트워크는 트래픽이 증가하고 메일 서버는 여전히 스팸메일에 의해 노출되어 있다.

2.2. 애플리케이션 게이트웨이

애플리케이션 게이트웨이방식[2]은 OSI 7 레이어의 애플리케이션 레이어에 해당되는 데이터 영역의 패킷만을 검증하는 방식을 지원한다. 즉 클라이언트에서 서비스 요청(Telnet, Http, Ftp)이 들어오면 파이어월에서 애플리케이션의 검증(Telnet Gateway, Ftp Gateway등의 검증을 통함)을 거쳐 목적 시스템으로 접속되는 방식이다. 애플리케이션 게이트웨이는 실제 데이터 확인을 통한 강력한 보안이 가능하다는 장점 이면에 속도가 느리다는 단점을 가지고 있다. 본 시스템 역시 메일 정책을 수행하기 위해 데이터까지 확인하는 애플리케이션 서버의 한 종류라고 할 수 있다. 본 시스템은 느린 속도를 극복하고자 커널 레벨에서의 구현을 시도하였다.

3. SSG

SSG는 외부 네트워크와 내부 네트워크 사이에 위치하며 이 사이를 오가는 모든 패킷은 SSG를 통과하게 된다.

SSG에서는 그림 1과 같이 SMTP로 접속하려는 패킷을 가로채어 자신과의 가상 연결을 설정하여 데이터를 읽고 내용을 확인한 후 메일 정책에 따라 처리하게 된다.

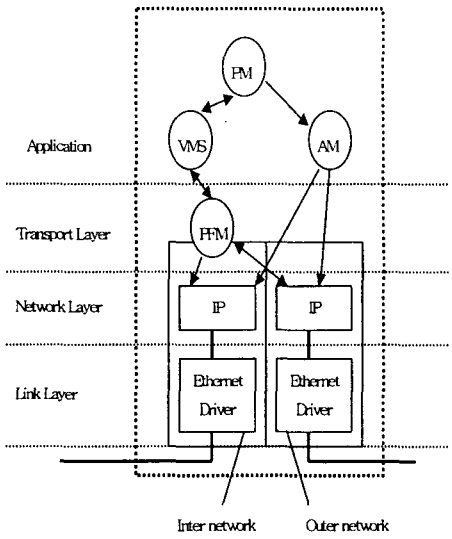

그림 1 SSSG의 기본 구조

- PFM(Packet Forwarding Manager)

IP 레이어에서 검사된 모든 TCP 패킷은 PFM 으로 올라온다. PFM은 Transport Layer의 TCP 속에 위치한다. 이곳에서 SMTP 가 아닌 패킷은 바로 내부 망으로 포워딩 되며 SMTP의 경우 가상연결을 만들고, 데이터를 VMS 로 전송한다. PFM 은 커널 레벨에 존재한다.

- .VMS(Virtural Mail Server)

PFM으로부터 받은 SMTP 데이터에 응답하며 메일 서버의 역할을 한다. 완전한 메일을 받아들여, PM으로 전송한다.

- PM(Policy Manager)

VMS가 접속하여 얻어진 메일을 받아 정책에 따라 적절한 AM을 선택하여 실행한다.

예를 들면, '제목에 특정 키워드가 포함되거나 내용에 특정 키워드가 포함되면 메일을 폐기하고, 로그를 기록한다.', '몇 회 이상의 제거 대상 메일을 보낸 주소에 대해서 블랙리스트에 등록하고 관리자에게 경고한다.' 등과 같은 정책을 들수 있다.

- AM(Action Module)

정책에 따라 실행될 여러 대응들이다.

예를 들면, 포워딩, 리플라이, 폐기, 관리자에게 경고 등이 있다.

4. SSG의 구현

본 시스템은 크게 커널 부분과 에이전트 부분 두

부분으로 나누어서 구현하였다. 시스템 성능 향상을 위해 패킷 감시를 커널 레벨에서 구현하였고, 이후 시스템 확장성을 위해 SMTP에 관련한 부분을 독립적으로 에이전트 형태의 애플리케이션으로 구현하였다.

4.1. 커널 부분

커널에서 감시 하는 특정 포트를 목적지로 하는 패킷을 자신의 에이전트와 통신하게 하는 기능을 구현하기 위해 다음과 같은 방법을 이용하였다.

ㄱ. 커널에서 TCP 패킷에 한하여 포트를 검사한다.

ㄴ. 감시대상 포트일 경우 포워딩 대신에 자신의 패킷처럼 상위 레이어로 처리한다.

ㄷ. 게이트웨이에서 감시하는 포트와 같은 번호로 대기 중인 에이전트가 패킷을 받아서 정책 처리한다.

위와 같은 프로세스로 시스템을 구축하였다. 그러한 결과를 얻기 위해선 원목적지의 호스트처럼 응답을 해줄 필요가 있다.

그림 2에서 파일들은 리눅스 커널 2.4.2 버전의 소스 코드 중 에서 ../net/ipv4 하위에 존재하는 파일이다. 이 파일들은 원하는 결과를 얻기 위하여, 다음과 같이 수정되었다.

- ip_input.c의 ip_rcv_finish() 함수 부분:

하위 레이어로부터 받은 패킷이 IP 레이어로 넘어와서 체크섬검사와 패킷검사를 마치고 난 부분이다. 패킷이 감시중인 포트(SMTP)일 경우 원래의 주소를 저장한다. IP 주소를 localhost로 바꿔, 패킷이 포워딩이 아니라, 상위로 레이어로 전송되도록 한다.

- ip_ouput.c의 ip_ouput() 함수 부분:

IP 패킷 작성을 끝내고 하위 레이어로 패킷을 보내는 부분이다. client에게 목적 호스트가 응답하는 것처럼 하기 위해 IP를 client의 목적 호스트 IP 로 바꾸고, 체크섬한다.

- tcp_ipv4.c의 tcp_v4_send_check() 함수 부분:

TCP 연결이 성립된 이후, 데이터를 주고받는 과정에서, 패킷 생성 시 마지막 단계부분이다. IP 레이어에서 목적호스트의 IP가 바뀌면, TCP 수도 헤더(pseudo header)가 변하므로, 체크섬 값이 변하게 된다. 이것을 수정하도록 하기 위해, 체크섬을 맞춘다.

- *tcp_ipv4.c*의 tcp_v4_send_synack() 함수 부분:

이 부분은 TCP 연결이 성립되는 과정에서 주고받는 패킷생성의 마지막 부분이다. 이 부분 역시 TCP 수도 헤더(pseudo header)의 내용에 맞추어 체크섬을 하여준다.

수정 된 커널에 의해 패킷은 그림 2와 같이 처리된다.

1) 네트워크 레이어(network layer): 들어오는 패킷을 검사하여 TCP 패킷이고 감시 대상 포트일 경우, 패킷의 목적지가 변경되어 트랜스포트 레이어로 보내어진다.

2) 트랜스포트 레이어(tranport layer): SYN.ACK(혹은 ACK) 패킷 생성

3) 네트워크 레이어(network layer): source IP를 원목적지 IP로 바꿔서 전송한다.

4) ACK를 받으면 커넥션 연결된다.

5) 이후 DATA를 받아도 같은 방식으로 주고 받는다.

클라이언트는 ip_input.c에서 라우팅되어 점선처럼 서버와 통신하고 있다고 생각하지만, 수정된 파일들은 다음과 같이 작동하여 게이트웨이와 실선으로 통신하고 있는 것이다.

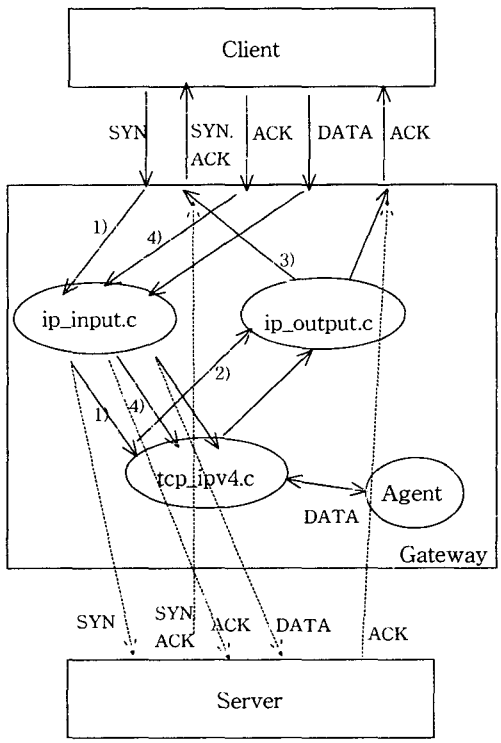

그림 2 리눅스 커널소스 수정안

4.2. 에이젼트

C로 구현된 에이전트 부분은 그림 1에서처럼 VMS와 PM, 그리고 AM으로 나뉜다.

수정된 커널에 의해 올라오는 데이터는 VMS와 통신하여 데이터를 받는다. VMS는 실제 sendmail 프로그램처럼 반응해야 하며, sendmail의 모든 명령어를 처리하도록 하여, 실제로 메일을 직접 받는다.

받아진 메일은 PM으로 보내어 지며, 정책에 맞게 처리 하여 포워딩이나 폐기 등의 적절한 액션을 선택하여, AM을 실행시킨다.

4.3. 장점 및 활용

본 시스템의 가장 큰 특징을 두 가지로 요약할 수 있다.

첫 번째, 게이트웨이에 존재 한다는 것이다. 네트워크의 게이트웨이에서 네트워크 전체에 대한 메일 감시가 가능하다. 즉, 같은 내용이 반복해서 수십 통에서 수백 통이 각각의 서버로 전송되는 스팸메일의 경우 게이트웨이에서 차단하므로, 내부 네트워크의 부하를 방지하고, 또 같은 메일을 각 서버에서 일일이 필터링 할 필요가 없다.

두 번째는 완전한 연결을 맺은 후 메일을 검사 한다는 것이다. 이것은 큰 의미가 있다. 단순히 몇몇 패킷을 보고 헤더의 내용으로 감시하는 것이 아니라 메일 전체 데이터를 이용하여 정책을 관리할 수 있다는 것이다. 메일 내용의 키워드 검색을 할 수 있음은 물론, 바이러스 검사까지 실제 메일서버가 받기 전에 처리 하여 통제할 수 있다. 또한 이러한 방식은 다른 용도의 시스템으로의 확장도 용이 한다.

5. 결론 및 향후 계획

본 시스템은 게이트웨이 단에서 SMTP 프로토콜을 이용한 전자 우편 서비스를 감시하며, 필터링 및 적절한 정책을 수행하는 체제이다.

각 서버에서 일일이 전자 우편에 대한 정책을 수행하는 것보다 효율적으로 게이트웨이에서 관리하므로, 네트워크와 각각의 메일 서버의 부하를 줄이는데 기여할 것으로 본다. 또한 메일 서버가 복수 개 존재하는 네트워크에서 메일 정책을 중앙 집중적으로 처리 할 수 있게 되어 효율성이 증대할 것이다.

커널 레벨에서의 패킷 감시는 일반 애플리케이션보다 빠르게 동작하여 효율성을 높일 수 있으며, 패킷 감시 기능만을 모듈로 구현하여 어떤 모듈을 만들어 접목 하느냐에 따라 타 분야로의 응용을 가능케 한다. 즉, 현재 구현된 커널만으로도 TCP를 이용하는 모든 통신에 대한 감시를 할 수 있으며, 약간의 수정작업을 더 하면 UDP 혹은 다른 프로토콜까지 감시 할 수 있다. 단순히 패킷의 주소만이 아닌 데이터의 내용을 받아보고 정책을 수행할 수 있다.

이 독립적인 커널 모듈은 많은 다른 응용을 가능하게 할 것으로 본다. 예로, TCP의 sync flooding 공격을 막는 시스템 또한 추가적인 수정으로 가능하다. 본 게이트웨이가 완전한 TCP 연결이 확립되는 것을 확인하기 때문에 sync flooding 공격 기법으로 네트워크 내부의 호스트를 공격하는 것을 차단할 수 있다.

아직은 TCP에만 한정되어 있고, SMTP에 대해서 정책을 수행하는 시스템이지만, 연구 개발 이후엔 게이트웨이 내부의 네트워크를 보호하는 통합 보안 시스템으로 발전할 수 있을 것이다.

참고문헌

[1] 출원인: 주식회사 데이콤 정규석, 발명자: 정연배, 공개번호: 특2002-00011, 출원번호: 10-2000-00354, "유령 아이디를 이용한 스팸 메일 방지 방법", 대한민국특허청(KR)

[2] 한국 썬 마이크로 시스템즈 보안 기술 문서, http://kr.sun.com/service/techdocs/0012/000143.html

[3] Jon Crowcroft, Iain Phillips, "TCP/IP and Linux Protocol Implementation", WilleyComputer Publishing

[4] 이귀영, "Linux Kernel Programming", 글로벌