제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

메일 컨텐츠 탐지를 위한 침입 탐지 시스템의 확장에 관한 설계 및 구현

한영주*, 김희승**, 정태명*
*성균관대학교 전기전자 및 컴퓨터 공학과
**성균관대학교 컴퓨터 공학과
e-mail : {yjhan, hskim }@imtl.skku.ac.kr,
and tmchung@ece.skku.ac.kr

Design and Implementation of the Extended Intrusion Detection System for Mail Contents Probing

Young-ju Han*, Hee-seung Kim**, and Tai-myoung Chung*
*Dept. of Electrical and Computer Engineering, Sungkyunkwan University
**Dept. of Computer Engineering, Sungkyunkwan University

요 약

인터넷이 발전함에 따라 기업의 업무, 커뮤니케이션 등이 온라인으로 전환되고 있으며, 정보 전달의 통로로써 전자 메일의 사용이 나날이 늘고 있다. 이에 따라 전자 메일을 통한 바이러스, 스팸 광고 등 메일의 컨텐츠를 이용한 공격에 의한 피해가 심각한 수준에 이르고 있다. 현재 방지 대책으로는 백신이나 스팸 메일 차단기 등을 통해 방지 기능을 제공하고는 있으나 이는 사용자의 의지에 의존적이며, 개개 시스템에 한정되는 한계가 있다. 따라서 사용자의 의지와 무관하게 네트워크 차원에서 내부 네트워크를 보호하기 위한 방지 대책이 필요하며, 이에 본 논문에서는 기존의 침입 탐지 시스템을 확장하여 메일 컨텐츠를 탐지할 수 있는 확장된 침입 탐지 시스템을 제안한다.

1. 서론

인터넷이 급속히 확산되고 발전된 지금, 인터넷을 기본으로 하여 중요한 통신 수단으로 자리 잡은 전자 메일 서비스는 현재 바이러스 유포의 통로로, 혹은 스팸 메일이라는 불법 광고를 위한 통로로 악용되는 부작용을 겪고 있는 현실이다[1]. 바이러스 배포용 메일의 경우는 사용자 컴퓨터를 파괴하여 정보 손실 등을 유발하며, 스팸 메일의 경우는 많은 사용자에게 무차별적으로 전송되기 때문에 네트워크 자원의 손실을 가져온다. 현재 백신이나 스팸 메일 차단기 등을 통해 방지 기능을 제공하고 있으나 이는 사용자의 의지에 의존적이며, 개개 시스템의 보호에 한정되는 한계를 가지고 있다. 따라서, 메일의 컨텐츠를 이용하여 내부로 유입되는 공격으로부터 조직의 내부 네트워크를 일괄적으로 보호할 수 있는 시스템이 필요하다.

본 논문에서는 이러한 취지에서 기존에 개발하였던 침입 탐지 시스템인 Secure Fortress를 메일 컨텐츠 탐지를 위하여 확장한 Extended Secure Fortress를 설계 및 구현하였다. Extended Secure Fortress는 기존의 구성을 그대로 유지하며 메일 탐지 시스템인 MCPS(Mail Contents Probing System)을 추가한 시스템이다. MCPS는 전자 메일을 이용하여 이루어지는 각종 스팸 메일, 정크 메일, 바이러스 유포 등 메일 컨텐츠를 이용하는 외부 공격을 미리 탐지하여 그 피해를 줄이는 것이 목적이다.

본 논문은 총 6장으로 구성되어 있다. 2장에서는 침입 탐지 시스템의 개요와 기존에 개발했던 Secure Fortress에 대해 간단히 살펴보고 3장에서는 확장된 침입 탐지 시스템인 Extended Secure Fortress에 대해 살펴 본다. 4장에서는 MCPS의 설계 및 프로세스 구성도에 대하여 논하고, 5장에서는 실제 어떻게

구현되었는지를 살펴본 후 마지막 6장에서 결론을 내린다.

2. 관련 연구

2.1 침입 탐지 시스템

침입이란 컴퓨터 시스템 혹은 네트워크에 불법적으로 접근하거나 시스템을 오용 또는 남용하는 행위를 말하며, 이는 컴퓨터가 사용하는 자원의 무결성, 비밀성, 가용성을 저해하는 일련의 행위들로 구성된 집합이라고 정의할 수 있다. 침입 탐지 시스템(Intrusion Detection System)은 이러한 침입을 목적으로 특정 시스템에 불법적으로 접속하여 시스템을 사용, 오용, 남용하는 것을 조기에 감지하여 실시간 처리가 가능하도록 하는 시스템이다[2]. 침입 탐지 시스템은 침입 탐지 모델 기반의 분류 방법에 따라 다음과 같이 나눌 수 있다[3].

■비정상적인 침입 탐지 기법

비정상적인 침입 탐지 기법은 감시되는 정보 시스템의 일반적인 행위들에 대한 프로파일을 생성하고, 이로부터 벗어나는 행위를 분석하는 기법으로, 통계적인 자료에 근거한 기법, 특징 추출에 의존하는 기법, 예측 가능한 패턴 생성 기법 등으로 나뉠 수 있다.

■오용 침입 탐지 기법

오용 침입 탐지 기법은 과거의 침입 행위들로부터 얻어진 지식으로부터 이와 유사하거나 동일한 행위를 분석하는 기법으로, 조건부 확률을 이용한 기법, 전문가 시스템, 상태전이 분석 기법, 키-스트로크 관찰 기법, 모델에 근거한 기법 등으로 나뉠 수 있다.

2.2 Secure Fortress

Secure Fortress란 연구실에서 구현한 침입탐지 시스템(Intrusion Detection System)으로써, 호스트 및 네트워크 기반의 침입 탐지를 수행하며 웹 기반의 관리 인터페이스를 제공하여 효율적이고 사용하기 편리한 시스템이다. Secure Fortress는 다음과 같은 시스템 구성을 가진다.

■ **WMI (Web-based Management Interface)**

전체 시스템에 대한 보안관리 기능 수행을 위한 작업 인터페이스를 제공한다.

■ **MAC (Multi-Agent Coordinator)**

다중 에이전트 관리자로 지칭하며, 감시대상 네트워크에 분산 설치되어 있는 다수의 에이전트 시스템들을 중앙 관리하는 기능을 수행한다.

■ **NSMA (Network Security Monitoring Agent)**

정의된 규칙을 기반으로 네트워크 오용을 탐지하는 오용탐지 침입탐지 에이전트이다. 네트워크 보안감시 에이전트는 단일 감시대상 네트워크 상에서 발생하는 패킷 정보를 수집하고, 침입 분석하는 기능을 수행하며, 침입 판정이 된 보안위반 사건에 대해서는 MAC으로의 통보 기능을 수행할 뿐만 아니라 통합 침입 분석을 위하여 MAC에 의해 설정된 보안 이벤트들은 MAC으로 보고한다.

■ **HAA (Host Audit Analyzer)**

HAA는 비정상적인 침입 탐지 기법을 기반으로 하는 침입 탐지 에이전트로써, 대상 호스트가 생성하는 로그정보로부터 보안관련 감사 정보를 수집하고 이를 분석하여 사용자의 비정상적 행위을 탐지하여 이를 MAC으로 통보한다. 이는 통합 침입분석 기능 지원을 위하여 정의된 보안 이벤트를 MAC으로 전달한다.

3. 메일 컨텐츠 탐지를 위한 침입 탐지 시스템의 확장

본 논문에서는 전자 메일의 컨텐츠 탐지를 위하여 기존의 Secure Fortress를 확장한 Extended Secure Fortress에 대해 논할 것이다. Extended Secure Fortress는 2.2절 에서 설명했던 각 시스템 구성은 그대로 유지하였으며, 컨텐츠 탐지를 위하여 MCPS를 추가하였다.

Extended Secure Fortress를 이용한 컨텐츠 탐지는 하나의 시스템으로 내부 네트워크 내의 모든 메일 서버를 대상으로 유입되는 메일을 대상으로 오용 메일을 탐지하여 대처할 수 있기 때문에 사용자 및 관리자에게 편리함을 제공하며, 사용자가 일일이 전용 바이러스 백신이나 스팸 메일 차단기 등의 소프트웨어를 이용하여 검사할 필요가 없기 때문에 추가비용이 들지 않는 장점이 있다.

3.1 MCPS(Mail Contents Probing System) 개요

MCPS는 정의된 규칙을 기반으로 전자 메일의 오용된 컨텐츠 탐지를 위한 시스템으로써, 외부로부터 유입되는 전자 메일을 탐지하여 메일의 보안 위반 여부를 검사 통보하는 시스템이다.

MCPS의 각 기능은 다음과 같다..

■ **MCPM (Mail Contents Probing Master)**

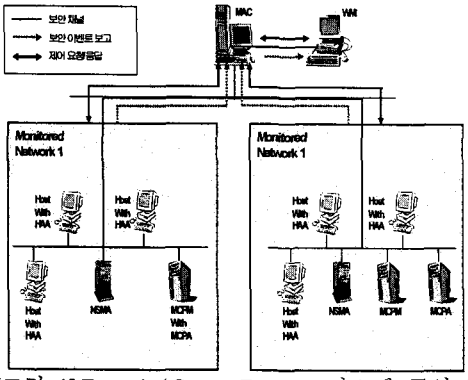
내부 시스템의 메일 서버로 들어오는 모든 메일을 수집하여 해당 메일의 규칙에 따른 컨텐츠 검사를 위해 MCPA에 의뢰하고 결과를 수신받아 MAC으로 보고한다.

■ **MCPA (Mail Contents Probing Agent)**

MCPA는 MCPM의 백 엔드(Back End)에서 동작하며, MCPM으로부터 수신한 SMTP 데이터에서 컨텐츠를 추출하고 컨텐츠 별로 보안 위반 사항을 점검한다. 첨부 파일을 대상으로 바이러스를 검사하며, 메일 제목 및 내용을 대상으로 하여 스팸 메일 여부를 검사한다. 마지막으로 검사 결과를 MCPM에게 통보한다.

MCPS를 추가한 전체 Extended Secure Fortress의 시스템 구성도는 [그림 1]와 같다. [그림 1]에서 보는 바와 같이 MAC과 에이전트 사이에는 MAC에서 각각의 에이전트로의 탐지를 위한 룰 설정 및 암호화 방식 등의 환경 설정을 위한 제어 채널과 각각의 에이전트로부터 MAC으로의 보안 이벤트 보고를 위한

트랩 채널를 가진다. 각각의 채널은 암호화되어 MAC과 에이전트들 간에 오가는 데이터들을 보호할 수 있다. 또한, MCPM과 MCPA는 하나의 서버에 같이 존재하거나, 각기 다른 서버에 존재할 수 있다.

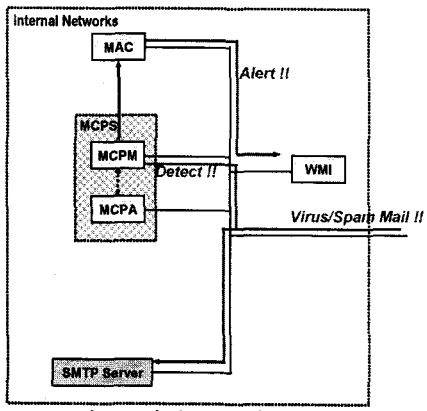


[그림 1] Extended Secure Fortress 시스템 구성도

3.2 컨텐츠 탐지 과정

Extended Secure Fortress를 이용한 컨텐츠 탐지 과정을 살펴보면 [그림 2]와 같다.

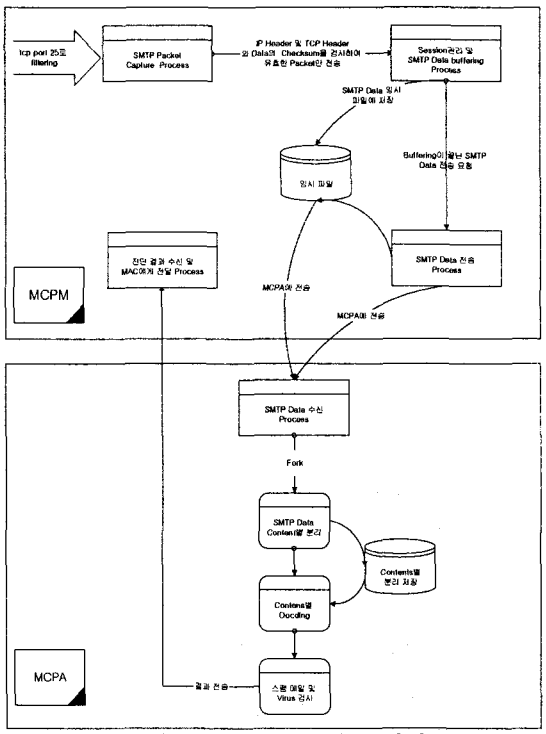
내부 SMTP 서버로 유입되는 SMTP 패킷을 중간에 위치한 MCPS에서 수집 및 탐지하여 보안 규칙에 어긋난 경우 MAC에게 보안 이벤트를 보낸다. 보안 이벤트를 받은 MAC은 이를 WMI에 보내고, 규칙에 따라 대응을 하게 된다. 그 대응 방법으로는 사용자 및 관리자에게 통보, 해당 메일 삭제 등이 있다.



[그림 2] 컨텐츠 탐지 과정

4. MCPS의 설계 및 구성

MCPS에서의 컨텐츠 탐지를 위한 전체 프로세싱 과정은 위한 과정은 [그림 3]와 같다. MCPM과 MCPA는 각각의 기능에 따라 여러 모듈로 구성되어 있다. 다음은 각각의 세부 모듈을 살펴보고자 한다.



[그림 3] MCPS 프로세싱 과정

4.1 MCPM의 세부 기능 모듈

■ ***네트워크 패킷 수집 모듈***

내부 네트워크로 유입되는 패킷 중 TCP의 목적지 포트 번호가 25이고 목적지 IP 주소가 관리 대상인 메일 서버의 주소인 경우 해당 SMTP 패킷을 수집한다.

■ ***SMTP 세션 관리 모듈***

현재 네트워크 상에 동시에 존재하는 여러 SMTP 세션을 관리 대상으로 한다. 세션 관리 방법은 다음과 같다.

첫째, 수집한 패킷에 대해서, IP 헤더 체크섬(checksum), TCP 헤더 및 페이로드(payload)에 대한 체크섬을 수행한 결과, "invalid" 패킷은 폐기한다[4]. 둘째, 수집한 패킷에 대해서, TCP 헤더의 플래그가 SYN인 경우, 새로 세션을 생성하고, RST나 FIN인 경우, 해당 세션을 삭제한다. 셋째, 수집한 패킷에 대해서, 페이로드가 존재할 경우, 해당 세션의 마지막 저장된 순서 번호(sequence number)를 검색하여, 현재 수집된 패킷의 순서 번호와 비교하여 현재 수집된 패킷의 순서 번호가 작은 경우, 재 전송된 패킷으로 간주하고 폐기한다.

■ ***SMTP 데이터 수집 모듈***

각 세션별로 SMTP 명령어를 포함한 모든 SMTP 데이터를 파일에 저장한다.

■ ***MCPA와의 통신 모듈***

한 세션에 대하여 수집이 끝난 SMTP 데이터를

MCPA에 전송한다

■ ***MAC과의 통신 모듈***

MCPA로 수신한 바이러스나 스팸 메일 정보를 보안 이벤트 채널을 이용하여 MAC에게 통보한다.

4.2 MCPA의 세부 기능 모듈

■ ***MCPM와의 통신 모듈***

MCPM으로 부터 SMTP 데이터를 수신하고, 처리 후 결과를 통보한다.

■ ***SMTP 데이터의 컨텐츠 별 분리 및 디코딩 모듈***

수신 받은 SMTP 데이터를 컨텐츠별로 분리한다. 즉, To 정보, From 정보, 메일 제목, 내용, 첨부 파일별로 분리한다. 분리 후 각 컨텐츠 별 MIME 헤더를 분석하여 헤더에 명시된 인코딩 방식으로 각각을 디코딩하여 컨텐츠의 본 속성으로 복원한다. 이러한 디코딩 방식에는 7bit, 8bit, binary, base64, quoted printable 방식 등이 있다[5].

■ ***바이러스 검사 모듈***

디코딩을 완료한 첨부파일을 대상으로 바이러스 검사를 수행한다. 바이러스 엔진은 공개 소스인 clamav를 사용하였다.

■ ***스팸 메일 여부 판정 모듈***

미리 설정된 스팸 메일 관련 룰을 기반으로 메일 from 정보, 제목, 내용을 대상으로 스팸 여부를 검사한다.

5. MCPS 구현

5.1 개발환경

- 운영체제 : Solaris Sparc 2.7
- 개발 언어 : gcc 2.95.3 release
- MCPM 패킷 수집 라이브러리 : libpcap 0.7
- MCPA 안티 바이러스 엔진 : clamav-0.15

5.2 구현

모듈 구성에 있어서 MCPM의 경우, 프로세스의 처리 부하가 네트워크 패킷 수집에 영향을 미치기 때문에, 데이터 처리 프로세스가 네트워크 패킷 수집 프로세스에 영향을 미치지 않게 하기 위하여 멀티 쓰래드로 구성하였다. MCPA의 경우, MCPM의 복수의 검사 요청을 실시간으로 처리할 수 있도록 fork 함수를 사용하여 멀티 프로세스로 구성하였다. 즉, 4장에서 설명한 각각의 기능 모듈에 대하여 MCPM은 쓰래드로, MCPA는 사용자 정의 함수로 구현을 하였다. MCPM의 경우 쓰래드간 통신으로 메시지 큐를 사용하였다. MCPA의 경우 바이러스 검사를 위해 사용하는 clamav는 공개 소스로써, 연동을 위해 약간의 수정을 하였다. MCPM의 주요 쓰래드 설명은 [표 1]에, MCPA의 주요 함수는 [표 2]에 나타내고 있다.

[표 1] MCPM의 주요 쓰래드 설명

쓰래드 명	설명
pcap_handler	SMTP 패킷 수집 및 무결성 검사
packet_analysis_th	세션 관리 및 데이터 버퍼링
mac2Trap_th	MAC과의 보안 이벤트 보고 채널
mac2Ctrl_th	MAC과의 제어 정보 채널
mcpa2Send_th	MCPA에게 수집한 SMTP 데이터 전송
mcpa2Recv_th	MCPA로부터 검사 결과 수신

[표 2] MCPA의 주요 함수 및 쓰래드 설명

함수 명	설명
mcpa_doit	MCPM으로부터 SMTP 데이터 수신
send_result	처리 결과를 MCPM에 전달
cmd_to	SMTP 세션 "to" 명령어 처리
cmd_from	SMTP 세션 "from" 명령어 처리
cmd_data	SMTP 세션 "data" 명령어 처리 메일 본문 추출
cmd_quit	각 메일 컨텐츠를 대상으로 바이러스 탐지 및 스팸 메일 탐지 수행
separator_contents	메일 본분으로부터 첨부 파일 추출
decode_base64	base64로 인코딩된 컨텐츠를 디코딩
decode_qp	quoted Printable로 인코딩된 컨텐츠를 디코딩
decode_xbit	7bit, 8bit로 인코딩된 컨텐츠를 디코딩
decode_bin	binary로 인코딩된 컨텐츠를 디코딩

6. 결론

스팸 메일, 정크 메일, 바이러스 유포등 메일의 컨테츠를 이용한 공격이 나날이 증가하고 있다. 현재 많은 방어 제품들이 나와있지만, 대부분 사용자 시스템에서 구동되는 제품들로써 사용자의 사용여부에 의존적인 한계를 가지고 있다.

본 논문에서 구현한 Extended Secure Fortress는 기존에 구현했던 침입 탐지 시스템인 Secure Fortress를 확장한 것으로써, 내부 메일 서버로 유입되는 메일을 대상으로 컨텐츠를 감시하여 바이러스 메일 또는 스팸 메일 여부를 탐지하여 적절할 대응을 할 수 있도록 하여 그 피해를 줄일 수 있게 한다.

앞으로의 연구에서는 스팸 메일 탐지에 있어서 현재는 스트링 패턴 매칭 방법이 갖는 한계를 극복하여 보다 완전한 메일 컨텐츠 탐지 모듈을 구현할 것이며, 또한 메일 컨텐츠 뿐만이 아닌 다른 컨텐츠를 대상으로 하는 탐지 모듈를 구상할 것이다.

참고문헌

[1] "2001년 정보화 역기능 실태 조사 보고서", 한국정보보호진흥원.

[2] Roger S. Pressman, "Software Engineering A Practltiners' Approach", 3rd Ed. McGraw Hill.

[3] D.E. Denning, "An Intrusion-Detection Model", In Processing of the IEEE Symposium on Security and Privacy, 1996.

[4] R. Braden et al., "Computing the Internet Checksum", RFC 1071, Sep. 1988.

[5] N. Borenstein et al., "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Sep. 1993.