FTS를 이용한 논리적 망 분리와 행위기반 탐지 시스템에 관한 연구

김민수* · 신상일* · 안정준* · 김귀남**

요 약

인터넷망을 이용한 정보 전달의 대표적인 수단인 이메일 서비스 등을 통한 보안위협이 급증하고 있다. 이러한 보안위협의 공격 경로는 첨부된 문서파일에 악성코드를 삽입하고, 해당 응용프로그램의 취약점을 이용하여 사용자의 시스템을 감염시키게 된다. 따라서 본 연구에서는 파일 전송과정에서 위장악성코드의 감염을 차단하기 위해, 논리적 망 분리인 FTS(File Transfer System)를 이용한 무결성 검증 및 행위기반 탐지 시스템을 제안하고, 기존의 보안기법과의 비교 및 검증하고자 한다.

A Study of Logical Network Partition and Behavior-based Detection System Using FTS

MinSu Kim* · SangIl Shin* · ChungJoon Ahn* · Kuinam J. Kim**

ABSTRACT

Security threats through e-mail service, a representative tool to convey information on the internet, are on the sharp rise. The security threats are made in the path where malicious codes are inserted into documents files attached and infect users' systems by taking advantage of the weak points of relevant application programs. Therefore, to block infection of camouflaged malicious codes in the course of file transfer, this work proposed an integrity-checking and behavior-based detection system using File Transfer System (FTS), logical network partition, and conducted a comparison analysis with the conventional security techniques.

Key words : Malware, FTS, APT, Signature and Behavior-based Detection System

접수일(2013년 8월 30일), 수정일(1차: 2013년 9월 16일), 게재확정일(2013년 9월 20일)

* 경기대학교 산업보안학과
** 경기대학교 융합보안학과(교신저자)

1. 서 론

인터넷망의 발전으로 전 세계가 하나의 네트워크로 연결되어, 전 세계의 각종 이슈 및 정보들을 쉽고 빠르게 접할 수 있게 되었다. 또한 국가의 공공기관 및 기업은 발전된 네트워크 환경의 의존도가 높아지고 있으며, 특히 정보를 전달하는 대표적인 수단인 이메일 서비스, FTP(File Transfer Protocol) 등을 통한 업무진행으로 신속성과 효율성을 극대화 할 수 있게 되었다[1].

그러나 이메일 서비스가 보편화 되면서, 사회공학적 기법(Social Engineering)을 악용한 다양하고 지능화된 보안위협이 급속도로 확산되고, 그 피해가 점점 커지고 있는 실정이다. 2012년 한해는 특정 대상을 목표로 문서의 취약점을 악용하여 조작된 문서파일을 송부하여 악성코드에 감염시키려는 타겟팅 공격인 APT(Advanced Persistent Threat)가 자주 발견되었다[2].

이렇게 전달되는 파일들은 PE(Portable Executable) 파일 구조이거나 스테가노그라피(steganography) 기법을 이용한 이미지 혹은 MP3 파일 또는 워드, ppt, pdf 등과 같은 문서로써 운영체제와 응용프로그램의 중간매체인 API(Application Programming Interface)를 이용하여 파일을 실행하게 되는데, 여기서 응용프로그램 취약점을 악용한 위장악성코드 공격이 이루어지게 된다. 위장악성코드 공격은 각종 문서 내에 악성코드를 은닉하여 내용을 확인하는 순간 악성코드에 감염되게 되어, 좀비 PC를 만들거나 개인정보 및 기밀정보를 유출하여 사회·경제적으로 매우 큰 손실을 야기하고 있다.

이러한 손실을 막기 위해 공공기관 및 기업은 보안위협에 대한 대책으로 2008년부터 국가 기관의 망 분리 사업이 진행되고 있다[3]. 하지만, 업무상 자료를 연계해야 하는 상황에서는 망 분리를 하기는 쉽지 않기 때문에 보안 대책으로 보안 업데이트 및 의심이 되는 이메일은 바로 삭제하도록 권장하고 있다.

따라서 본 연구는 파일전송을 통한 위장악성코드의 감염을 차단하기 위해 논리적 망 분리인 FTS(File Transfer System)를 이용한 무결성 검증 및 행위기반 탐지 시스템을 제안하고, 기존의 보안기법과의 비교 및 검증하고자 한다.

2. 관련연구

공공기관이나 기업 조직 내의 방화벽 등에 의해 직접적인 공격이 대부분 차단됨에 따라, 조직 내부를 공격하기 위한 방안으로 문서 내에 악성코드를 은닉시켜 이메일에 첨부하여 전달하는 방법이 많이 활용되고 있다[4]. SANS에서 발표한 효과적인 사이버 방어를 위한 중요 보안 컨트롤 Top 20으로 웹 기반 및 응용 소프트웨어의 취약점에 대하여 지적하였다[5].

이메일을 이용하여 문서파일인 워드, pdf 등으로 위장하면 실제 관련된 내용을 보여주지만, 그와 동시에 응용프로그램의 취약점을 이용한 악성코드가 설치되기 때문에, 사용자는 악성코드 설치 여부를 알아채기 어렵다. 이러한 이메일을 통한 공격을 예방하기 위하여 한국인터넷진흥원은 APT와 같은 지속적 공격과 업무와 관련된 스팸 메일의 특징이 특정사이트로의 접속을 유도하거나, 첨부파일을 열어보게 하는 등의 위장 방법을 사용하므로 관련 링크를 클릭하지 않도록 주의하여야 하며, 백신 및 OS에 대한 최신 보안업데이트와 실시간 감시기능을 활성화해야 한다고 권고하고 있다.

또한 이메일 대상의 악성코드를 탐지하기 위한 기법으로 기존의 보안위협 패턴 시그니쳐를 기반으로 악성코드 파일을 유니크(Unique)하게 식별하기 위해 사용되는 방법인 시그니쳐 방식과, 시스템의 룰과 패턴을 사용하여 알려지지 않은 악성코드를 탐지하기 위해 사용하는 기법으로 기존 유해 프로그램의 코드를 분석하여 향후 발생할 수 있는 보안위협을 막고자 하는 Heuristic 기술이 개발되었지만, 신규로 발생하는 보안위협과 지능적으로 변모하는 변종 보안위협에 대해 실시간으로 대응 할 수 없다는 문제점이 있다[6][7][8]. 반면, 행위기반 악성코드 탐지 기법은 정적 분석(static analysis)과 동적 분석(dynamic analysis)으로 구분되어지고, 동적분석은 악성 행위를 발견하기 위하여 프로그램의 실행을 감시하고, 추적하는데 주목적이 있다. 동적 분석은 정적 분석에 비해 PE 파일의 변경에 영향을 받지 않고, 자원별 접근형태를 정확히

확인할 수 있는 장점을 지니고 있다[9][10][11].

하지만 이러한 기법들은 사용자의 선택에 따라 혹은 실수에 의하여 얼마든지 악성코드에 감염될 수 있기 때문에 본 연구에서는 내·외부 망에서 전송되는 이메일 첨부파일에 대하여 논리적 망 분리와 행위기반 탐지 기법을 적용하여 기존의 기법의 단점을 보완하려 한다.

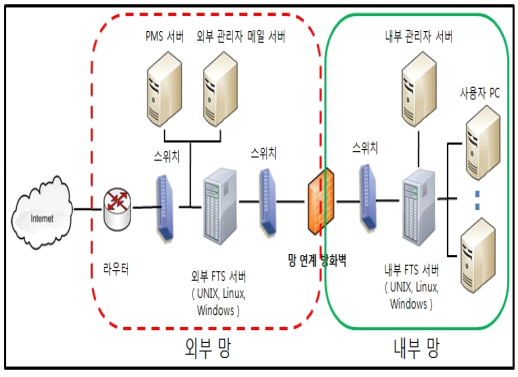
3. 제안하는 방법

본 논문은 제한적인 연구로써 산업기관의 네트워크 기반 논리적 망 분리 형태를 기본으로 한 FTS 행위기반 탐지 방안을 제안한다.

3.1 이미지변환 및 무결성 검출 시스템

(그림 1)은 FTS 구조의 이미지변환 및 무결성 검증 시스템으로, 외부망과 내부망을 망 연계 방화벽을 이용하여 논리적 망 분리를 하여 관리자에 의한 단방향 연결지향형태를 가지게 된다. 이때 PMS(Patch Management Server)에서 서버의 업데이트를 관리하게 된다.

외부 관리자 메일 서버에 수신된 이메일 첨부 파일인 문서를 FTS 서버에서 호출을 하여 pdf, jpg, png 등의 이미지 형태로 변환되어 웹 브라우저 상에서 확인할 수 있게 된다. 이미지로 변환 후 DRM(Digital Rights Management) 시스템 기술을 적용하여 암호화하여 내부 망으로 전달하게 된다.



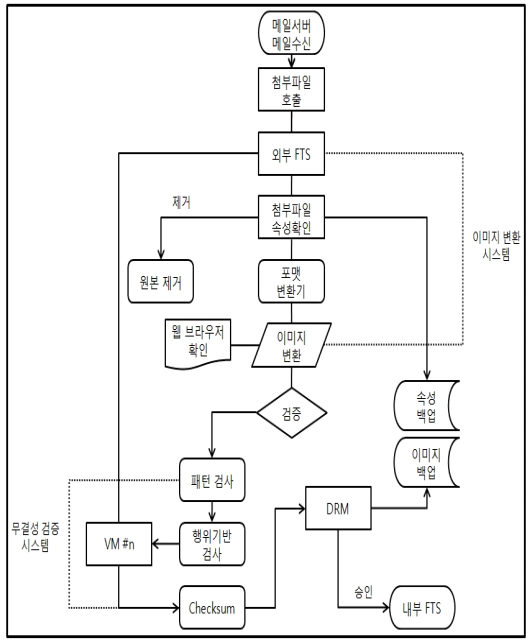
(그림 1) FTS 기반 이미지변환 시스템

또한 이메일에 첨부된 파일에 대한 검증 대상은 <표 1>과 같다.

<표 1> 첨부 파일 검증 대상

파 일	확장자
문서파일	HWP, DOC,DOCM,DOCX
	PPT, PPS, PPTX, PPTM
	XLS, XLSM, XLSX
PE 파일	scr, chm, exe
압축파일	zip, alz, rar
기타파일	eml

3.2 FTS 시스템 Flowchart



(그림 2) FTS 시스템 Flowchart

(그림 2)는 FTS 기반 이미지변환 및 무결성 검출 시스템의 운영 순서도로써, 관리자 메일서버에 수신된 메일의 첨부파일은 FTS 서버에서 실시간으로 호출하여 파일의 속성을 확인하게 된다. 이때 첨부파일의 속

성은 FTS에 백업을 하게 된다.

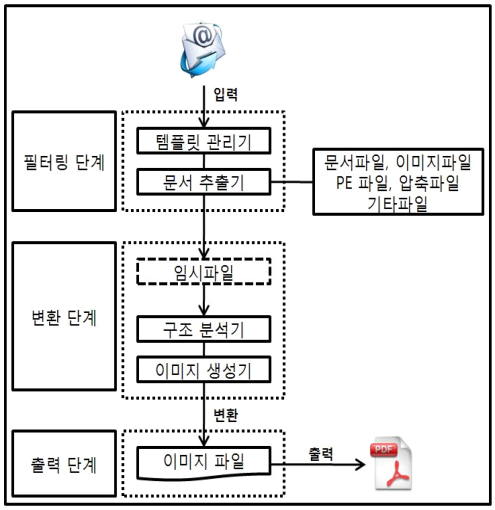
속성 확인 후 각종 이미지 포맷 변환기를 통하여 이미지로 변환하여 웹 브라우저 상에서 이미지를 확인할 수 있다. 또한 기밀 문서의 경우 문서열람을 제한하기 위하여 DRM 시스템 기술을 적용하여 이미지를 암호화 할 수 있다. 변환된 이미지는 FTS에 백업을 하게 된다.

이때 이미지 변환한 파일에 대한 무결성이 검증되어야만 내부 FTS의 승인을 할 수 있다. 이를 위하여 무결성 검증 수행을 하게 된다. 무결성 검증 엔진을 통하여 패턴검사, VM을 이용한 행위기반 검사 후 Checksum 기록을 하게 된다. 이 기록은 내부 FTS에서 Checksum과 비교하여 이미지파일의 변화를 체크하게 된다.

또한 포맷 변환기의 추가 기능으로 프린터를 제안할 수 있고, 내부망으로 이미지 전송을 위해 승인을 요청하고 승인이 이루어지면 암호화된 이미지파일을 내부망으로 전송하게 된다.

3.3 포맷 변환기[12]

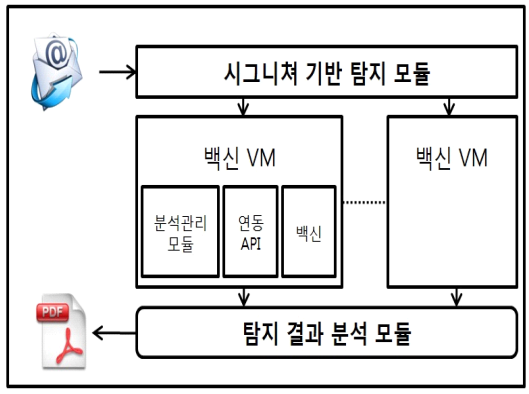
(그림 3)은 이미지 포맷 변환기로 호출된 첨부파일은 포맷 변환기에서 템플릿 관리기에서 속성을 확인하고 형태에 따라 문서를 추출하게 된다. 추출된 문서는 임시파일로 저장되어 구조 분석기와 이미지 생성기를 거쳐 원하는 이미지 파일로 출력되게 된다.



(그림 3) 포맷 변환기

3.4 시그니쳐 기반 탐지 시스템[4]

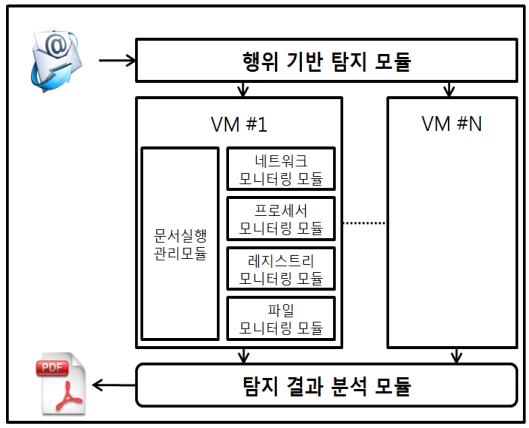
(그림 4)는 시그니쳐 기반 탐지 시스템으로 악성문서를 탐지하는 과정이다. 분석 대상 첨부파일별로 시그니쳐 기반 모듈은 분석을 요청하고 대상 파일을 스캔하여 악성여부를 판정 후 결과를 전달하는 방식이다.



(그림 4) 시그니쳐 기반 탐지 시스템

3.5 행위 기반 탐지 시스템[4]

(그림 5)는 행위 기반 탐지 시스템으로 시그니쳐 기반 방식에 비해 좀 더 복잡한 단계를 거쳐 악성여부를 판정하게 된다. 행위 기반 탐지 모듈은 문서파일을 해당 응용프로그램으로 실행하여 탐지 및 분석을 요청하고 시스템의 행위를 모니터링하게 된다.

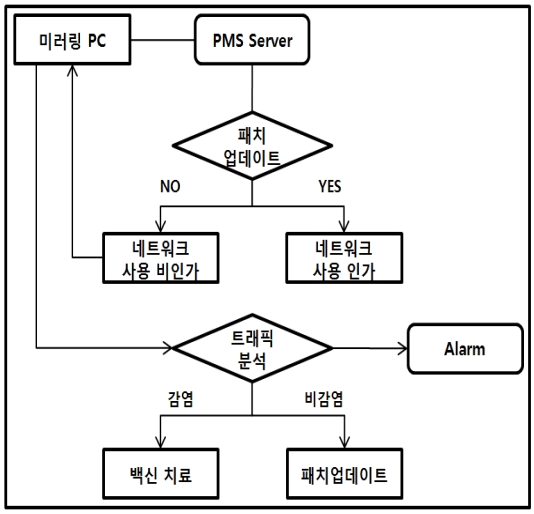


(그림 5) 행위 기반 탐지 시스템

3.6 패치관리시스템 서버 Flowchart[13]

(그림 6)는 패치관리시스템 Server의 운영 Flowchart로, 패치업데이트의 유무에 따라 네트워크 사용에 제한을 주게 된다. 네트워크의 제한을 받게 된 PC는 미러링 PC를 통하여 트래픽 분석을 하게 된다.

트래픽분석을 통하여 해당 PC의 이상유무를 확인하게 되고, 감염여부에 따라 치료 및 패치업데이트를 하게 된다. 또한 패치 업데이트에 대한 Alarm을 주게 된다.



(그림 6) 행위 기반 탐지 시스템

4. 악성코드 탐지 시스템 비교검증

지금까지 살펴본 악성코드 탐지 시스템과 일반 사용자용 Anti-Virus를 대상으로 시스템 간 비교검증을 실시하였다.

<표 2>를 보면, 일반 사용자용 백신의 경우 알려진 악성코드만을 탐지할 수 있고, 시그니쳐 기반 탐지 시스템의 경우는 PE 탐지 및 악성문서 탐지가 가능하나 백신과 같이 알려진 악성코드만을 탐지할 수 있다.

반면 행위 기반 탐지 시스템의 경우 새로운 취약점에 대한 탐지가 가능하나, 망 분리가 되어있지 않기 때문에 지능적인 공격에 노출되게 된다.

여기서 문서파일의 악성유무를 판단에 있어 응용프로그램의 버전에 따라 해당 프로세스의 스택 포인트를 포함한 레지스트리의 값들이 달라져, 문서내의 은닉된 악성코드의 위치 계산 결과가 달라져서 실행이 되지 않기 때문에 다양한 버전의 응용프로그램으로 확인해야 한다.

FTS는 망 분리된 네트워크 환경에 관리자 승인에 의한 행위 기반 탐지가 이루어지기 때문에, 내부망에 악성코드 감염이 어렵다.

<표 2> 악성코드 탐지 시스템 비교검증

	PE 탐지	악성문서 탐지	새로운 취약점 탐지	망 분리
백신	×	×	×	×
시그니쳐	○	○	×	×
행위기반	○	○	○	×
FTS	○	○	○	○

5. 결 론

본 연구는 정보보안 위협의 최초 감염이 가장 중요한 단계로 이를 예방하기 위한 탐지 시스템으로 FTS를 이용한 이미지 변환 및 행위기반 탐지 시스템을 제안하였다.

제안된 시스템은 외부망과 내부망을 망 연계 방화벽을 이용하여 논리적 망 분리를 하여 관리자에 의한 단방향 연결지향형태를 가지게 된다. 수신된 파일을 다운로드 받아 응용프로그램으로 열어서 내용을 확인하지 않고, pdf 또는 jpg,png 형태의 이미지로 변환하여 웹브라우저 상에서 확인하게 된다. 또한 망 분리를 기반으로 행위기반 탐지 기법을 사용하여 기존의 악성코드 탐지 및 차단을 위한 이메일 보안 시스템의 단점을 극복하였다.

FTS 시스템은 검증모드, 포워드모드, 탐지모드로 3가지 수행모드를 수행하게 된다. 검증 모드 단계에서는 메일의 첨부파일을 이미지화 시켜 웹브라우저

상에서 확인하고 악성 유무를 판단하게 되고, 수신을 하여야 하는데 악성 메일인 경우 관리자는 원본 파일의 악성코드를 치료하여 이미지화 시킨다. 포워드 모드는 최종 승인된 이미지 파일은 외부 FTS에서 연결 지향형이면서 단방향성으로 설정된 내부 FTS로 전달되게 된다. 탐지모드에서는 내부 FTS로 전달된 이미지 파일을 다시 한번 탐지하게 된다. 정상적으로 판단된 파일은 다시 원본 파일로 변환하여 최종적으로 사용자에게 전달되게 된다.

이와 같이 수행되는 FTS 시스템은 다른 악성코드 탐지 시스템에 비하여 망 분리된 네트워크 환경에 관리자 승인에 의한 행위 기반 탐지가 이루어지기 때문에, 내부망에 악성코드 감염이 어렵다는 장점을 지니고 있다.

참고문헌

[1] 유진호, 임종인, “스팸메일 관리피표 개선에 관한 연구”, 정보보호학회, Vol.19, No.3, pp.133-142, 2009.

[2] 국가정보원 외, “2013 국가정보보호백서”, p.67, 2013.

[3] 국가정보원, “2009 국가정보보호백서”, pp.66-67, 2009.

[4] 박춘식, “악성코드 은닉 문서파일 탐지를 위한 이메일 백신 클라우드 시스템”, 한국멀티미디어학회, Vol.13, No.5, pp.754-762, 2010.

[5] http://www.sans.org/critical-security-controls/spring-2013-poster.pdf.

[6] http://www.hauri.co.kr/customer/security/colum_view.html?intSeq=93&page=1.

[7] A.sung, J.Zu, P.Chavez and S.Mukkamala, "Static Analyzer for Vicious Executavles(SAVE)", 20th Annual Computer Security Applications Conference, pp.326-334, 2004.

[8] 김성우, 신재인, 방영환, “행위 기반 악성코드 탐지·차단시스템 개발”, 보안공학연구지원센터, Vol.9, No.2, pp.163-176, 2012.

[9] J.Bergeron, M.Debbabi, J.Desharnais, M.M.Erhioui, Y.Lavoie and N.Tawbi, "Static Detection of Malicious Code in Executable Programs", SREIS '01, 2001.

[10] S.G.Masood, Malware analysis for administrators, http://www.securityfocus.com/infocus/1780, 2004.

[11] 박남열, 김용민, 노봉남, “우회기법을 이용한 악성코드 행위기반 탐지 방법”, 정보보호학회, Vol.16, No.3, pp.17-28, 2006.

[12] 김성한, 이강찬, 민재홍, “XML 기반의 문서변환 시스템 기술 분석”, 한국전자통신연구원, Vol.17, No.3, pp.23-29, 2002.

[13] 김민수, 신상일, 김종민, 최경호, 이대성, 이동휘, 김귀남, “Reverse Proxy Group과 PMS를 이용한 멀티벡터(Multi-Vector) DDoS 공격 방어시스템 구축 방안, 한국융합보안학회, Vol.13, No1, pp.79-86, 2013.

[저 자 소 개]

김 민 수 (Min-Su Kim)

2004년 컴퓨터공학사
2012년 경호안전학석사
2013년 현재 경기대학교
산업보안학과 박사과정

email : fortcom@hanmail.net

안 정 준 (Chung-Joon Ahn)

1981년 행정학사
2004년 정책학석사
2013년 현재 경기대학교
산업보안학과 박사과정

email : ajj9000@hanmail.net

신 상 일 (Sang-Il Shin)

2004년 컴퓨터공학사
2007년 컴퓨터공학석사
2013년 현재 경기대학교
산업보안학과 박사과정

email : sishin69@hanmail.net

김 귀 남 (Kuinam J. Kim)

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 융합보안학과 교수

email : harap123@daum.net