2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

Unknown 웜바이러스 확산 방지를 위한 면역시스템 설계

김두현*, 임명현*, 오근탁*, 김판구*
*조선대학교 전자계산학과
e-mail:mindul@mina.chosun.ac.kr

The Design of Immune System for Blocking unknown Worm Virus Spreading

D.H. Kim*, M.H. Lim*, G.T. Oh*, P.K. Kim*
*Dept of Computer Science, Chosun University

요약

인터넷의 확산과 이용자의 급증으로 웜바이러스에 대한 문제가 최근에 크게 대두되고 있다. 스크립트형 웜바이러스의 경우 제작이 쉬워 누구나 몇 시간의 학습을 통하여 바이러스를 제작할 수 있다. 이러한 문제의 심각성은 최근 7개월 동안의 바이러스 통계에서도 나타나는데 전체 바이러스 중 평균 22.5%를 차지하고 있다. 이러한 웜바이러스를 차단하기 위해서 여러 가지 방법들이 사용되고 있으나 E-mail로 급속하게 퍼지는 웜바이러스의 확산을 차단하기 위해서 네트워크 기반의 시스템 보호방법이 요구되어지고 있다.

이에 본 논문에서는 알려지지 않은 웜바이러스로부터 내부 네트워크를 방어하기 위한 면역시스템을 제안한다. 자동화된 면역 시스템은 분산된 각각의 웜바이러스 탐지 시스템들이 새로운 바이러스 정보를 동적으로 공유할 수 있도록 하여 새로운 바이러스로부터 해당 시스템과 그 시스템이 속해 있는 내부 네트워크를 바이러스로부터 보호할 수 있도록 한다.

1. 서론

우리 나라는 경제협력개발기구(OECD) 회원국 가운데 광대역 인터넷 보급률이 압도적으로 높은 것으로 나타났다고 2001년 OECD 보고서가 밝혔을 정도로 인터넷이 빠르게 확산되고 있다. 이와 더불어 PC를 갖는 사용자가 늘어나고 컴퓨터 네트워크와 인터넷이 확산됨에 따라 컴퓨터시대의 역기능중의 하나인 컴퓨터 바이러스의 출현과 그 피해 또한 급증하고 있는 것이 사실이다.

최근에는 네트워크가 발달됨에 따라 공유된 네트워크 드라이브를 통하여 전파되는 바이러스가 많이 확산되고 있다. E-mail을 통하여 유포되는 바이러스는 1999년 초 이후 지속적으로 나오고 있음에도 불구하고 이에 대한 예방이 거의 이루어지지 않고 있어 여전히 많은 피해를 주고 있다. 그리고, 외국에서 바이러스가 발견된 지 몇 시간 뒤에 국내에서도 바로 발견되어 이제 바이러스의 문제는 국경을 초월하는 심각성을 보여주고 있다.

앞으로는 리눅스 바이러스와 개인휴대단말기, 이동 통신 기기 등 휴대용 통신 기기에서 활동하는 바이러스가 본격적으로 출현할 것이며 인터넷을 통해 전파되는 웜바이러스가 더욱 기승을 부릴 것으로 예상된다. 이런 문제에 대비하기 위하여 새로운 바이러스를 진단하고 그 정보를 내부 네트워크로 연결된 컴퓨터들이 다같이 공유할 수 있도록 하여 바이러스의 확산을 미연에 방지할 수 있는 면역 시스템에 대한 연구도 필요하다.

이에 본 논문에서 제안한 자동화된 면역 시스템을 이용하여 분산된 각각의 웜바이러스 탐지 시스템들이 바이러스 정보를 서로 동적으로 공유하여 바이러스로부터 해당 시스템이 속해 있는 네트워크를 바이러스로부터 방어할 수 있도록 하고자 한다.

2. 웜바이러스와 면역시스템

본 장에서는 그 동안 발견된 웜바이러스의 특징에 대하여 알아보고, 웜바이러스의 확산을 방지할 면역

시스템에 대하여 살펴본다.

2.1 스크립트형 웜바이러스

최근 급격히 증가하게 된 스크립트형 웜바이러스는 2001년도 통계를 보더라도 앞으로도 적지 않은 문제를 야기할 것으로 예상된다[5].

(표 1) 2001 바이러스 통계

Virus	Jan	Feb	Mar	Apr	May
File	60.0	78.2	74.2	43.1	95.2
Script	26.4	10.0	10.4	44.0	2.4
Macro	13.4	11.6	15.3	12.4	2.3
Boot	0.2	0.2	0.1	0.4	0.1

이러한 스크립트형 웜바이러스는 대부분 VBS (Visual Basic Script)로 작성되는데, VBS는 몇 시간의 학습을 통해서 바이러스를 제작할 수 있을 정도로 쉬운 스크립트 언어이기 때문에 많이 이용되고 있다[3].

2.2 VBS 웜바이러스의 특징

지금까지 발견된 VBS 웜바이러스 가운데 VBS.LoveLetter, VBS.SST@mm, VBS.Stages.A, VBS.LoveLetter.C, VBS.vbswg.gen 등의 바이러스를 분석하여 다음과 같은 특징을 발견할 수 있다.

웜바이러스가 작업을 수행하기 위해서는 먼저 객체를 생성하고 그 객체에 대한 메서드를 호출한다. 이때, 웜바이러스에 의해 생성되는 객체들은 Scripting.FileSystemObject, WScript.Shell, WScript.Network, Outlook.Application 등이 있다.

이러한 객체들 가운데 Outlook.Application은 Outlook이 설치된 시스템에만 존재하고 나머지 객체들은 WSH(Windows Script Host)가 설치되어 있는 시스템에 항상 존재한다. 대표적인 웜바이러스인 VBS.LoveLette의 네 가지 특징은 레지스트리를 조작하여 부팅시 자동실행하는 것과 E-mail을 통해 널리 퍼진다는 것, 특정한 파일을 찾아서 삭제하는 것, 그리고 악성 HTML 파일을 생성한다는 것이다. 각각의 특징별로 자세하게 살펴보면 다음과 같다[6,7].

① 레지스트리 조작

시작프로그램을 등록하는 레지스트리에 바이러스의 위치정보를 기록하여 부팅할 때마다 자동으로 실행되도록 하고 있다. 사용하는 객체와 메서드는 CreateObject와 RegWrite이다. 그리고, 바이러스가 조작하는 레지스트리는 아래와 같다.

-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

-HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

② 자동 메일 전송

Outlook에서 사용하는 WAB(Windows Address Book)라는 주소록 파일을 오픈하여 등록된 사용자들에게 바이러스를 첨부하여 자동 전송한다. 주로 사용하는 객체와 메서드는 CreateObject, WScript.Shell, Outlook.Application, GetNameSpace, AddressLists, RegRead, CreateItem이다.

③ 특정한 파일 검색, 복사, 덮어쓰기

사용자가 자주 이용하는 파일(jpg, mp2, mp3 등)을 하드디스크에서 찾아 덮어쓰거나 바이러스 자신을 같은 이름으로 복사한다. 여기서 사용하는 객체와 메서드는 GetFolder, GetExtensionName, OpenTextFile, GetBaseName, DeleteFile, CreateTextFile가 있다.

④ 악성 HTML 파일 전송을 통한 바이러스 감염

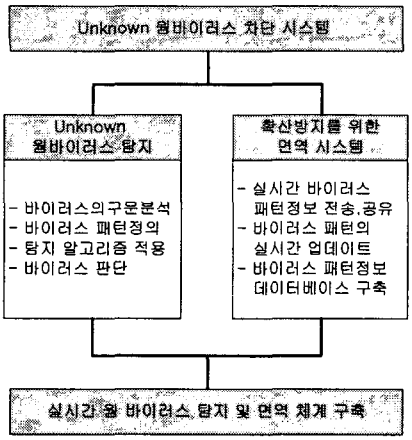
사용자가 mIRC를 이용하여 채팅을 하면 'Very Funny.HTM' 파일을 상대방에게 보내게 되는데 이때 상대방에게도 바이러스 감염된 파일을 실행하도록 유도해 결국 상대방의 시스템도 바이러스에 감염되게 한다.

3. 시스템 설계

본 장에서는 위에서 살펴본 웜바이러스를 탐지하고 그 확산을 미연에 예방할 수 있는 면역시스템을 설계한다.

3.1 시스템 구성

제안된 시스템은 (그림 1)과 같이 Unknown 웜바이러스 탐지 모듈과 면역시스템 모듈로 구분할 수 있다.

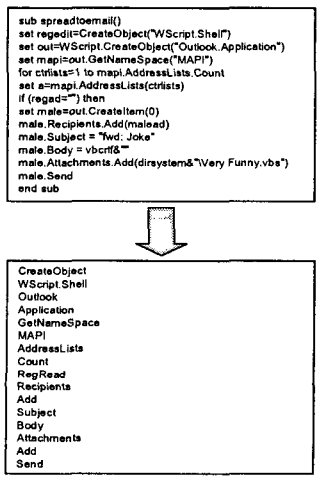


(그림 1) 시스템 구성

3.2 웜바이러스 탐지 알고리즘

실시간으로 웜바이러스를 탐지하기 위해 시스템은 부팅시 맨 처음 실행되어 시스템을 모니터링 하게 된다. POP3 서버를 통하여 메일이 오면 첨부파일을 검사하게 된다. 여기서 첨부파일인 VBS 파일을 Unknown 웜바이러스 탐지 모듈이 바이러스 여부를 검사하게 되는데 절차를 정리하면 다음과 같다.

① 바이러스 파일을 읽어들여 구문을 분석
② 미리 만들어진 패턴의 트리와 비교
③ 정의된 패턴일 경우에는 데이터베이스 추가 없이 로그기록에 남김
④ 새로운 패턴일 경우 패턴 데이터베이스에 추가
⑤ 내부 네트워크에 속한 다른 시스템에 바이러스 정보 전송



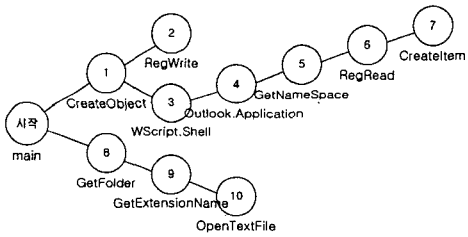
(그림 2) 바이러스 구문 분석

바이러스의 패턴트리를 구성하기 위하여 매핑 테이블을 (표 2)와 같이 작성하게 된다.

(표 2) 매핑 테이블

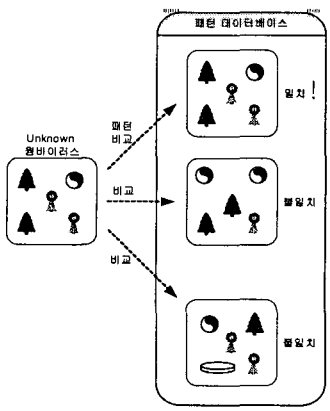
객체 또는 메서드	번호
CreateObject	1
RegWrite	2
WScript.Shell	3
Outlook.Application	4
GetNameSpace	5
RegRead	6
CreateItem	7
GetFolder	8
GetExtensionName	9
OpenTextFile	10
:	:
:	:

다음에는 작성된 매핑 테이블을 이용하여 패턴 트리를 (그림 3)과 같이 작성한다.



(그림 3) 바이러스 패턴 트리

여기에서 바이러스는 2.2절에서 VBS.LoveLetter 바이러스를 예로 들어 살펴본 바와 같이 네 가지 특징 중 한 가지만으로도 구성될 수 있고, 네 가지 특성 모두를 가질 수도 있다. 그러므로, 위의 패턴을 근거로 알려지지 않은 바이러스의 패턴과 패턴 DB의 패턴들을 비교하여 (그림 4)와 같이 바이러스 여부를 판단하게 된다.



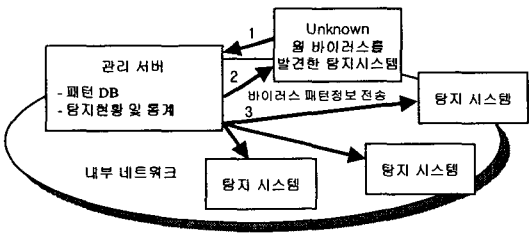
(그림 4) 패턴DB의 패턴과 비교

3.3 면역 시스템

일반 사용자의 대부분이 바이러스에 대한 마인드가 부족하고, 적절한 예방요령과 대처방법에 대하여 미숙하기 때문에 현재의 바이러스 엔진을 업데이트하는 수동적인 방법으로 바이러스를 퇴치하는 데는 문제가 있다고 볼 수 있다. 그러므로, 알려진 또는 알려지지 않은 바이러스를 진단하고 그 정보를 내부 네트워크로 연결된 컴퓨터들이 다같이 자동으로 공유할 수 있도록 하여 바이러스의 확산을 미연에 방지할 수 있는 면역 시스템이 필요하다.

앞의 탐지 모듈에서 탐지해낸 웜바이러스로부터 새로운 패턴을 추출하였다면, 데이터베이스가 구축된 서버에 패턴 정보를 전송하여 패턴 DB에 추가하도록 한다. 이와 동시에 탐지 모듈이 이미 설치되어 있는 내부 네트워크의 다른 시스템에도 패턴 정보를 즉시 전송하여 추후에 이와 동일한 패턴을 가진 웜바이러스가 첨부파일로 왔을 때 탐지 단계에서 빠르게 차단할 수 있게 된다.

네트워크에 기반한 면역시스템의 구성은 (그림 5)와 같다.



(그림 5) 면역시스템 네트워크 구성도

그러면 지금까지 살펴본 웜바이러스의 탐지에서부터 면역시스템을 통한 시스템 보호까지의 절차를 정리하면 다음과 같다.

① 1 단계

탐지된 알려지지 않은 웜바이러스 정보는 DB에 저장되기 위하여 적절한 자료구조로 변환되어 패턴 DB가 설치된 관리 서버로 보내어진다.

② 2 단계

분석된 바이러스 패턴은 관리서버의 데이터베이스에 저장되게 되고, 이 패턴 정보는 다시 맨 처음 바이러스 정보를 보내온 컴퓨터에 보내어 자신의 정보를 갱신한다.

③ 3 단계

맨 처음 바이러스 정보를 보내온 컴퓨터를 제외한 나머지 다른 컴퓨터들에게도 바이러스 패턴 정보는 전송된다. 그래서, 내부 네트워크에 종속된 모든 컴퓨터들은 동일한 바이러스로부터 면역력을 향상시키게 된다.

4. 결론 및 향후연구

본 논문에서는 인터넷을 통해 전파되는 웜바이러스에 대해서 알아보고, 웜바이러스의 확산을 막기 위한 면역시스템을 제안하였다.

제안된 시스템은 알려지지 않은 웜바이러스까지 탐지 가능하고, 새로운 웜바이러스로부터 내부 네트워크에 종속된 다른 시스템을 보호할 수 있다.

앞으로는 알려지지 않은 바이러스의 진단율을 더욱 높이기 위한 알고리즘에 대한 연구가 필요하며 또한, 바이러스의 행위를 탐지하여 바이러스를 진단할 수 있는 행위기반 바이러스 차단 시스템에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] Anil Somayaji, Steven Hofmeyr, Stephanie Forrest "Principles of Computer Immune System" Proceedings of the workshop on New security paradigms workshop, 1997, Pages 75~82.

[2] Jeff Kephart "Automatic Extraction of Computer Virus Signatures" Virus Bulletin International Conference, 1994, Pages 178~184

[3] Mark Kennedy "Script-Based Mobile Threats" Symantec AntiVirus Research Center, 2000

[4] Yoshiteru Ishida "The Immune System as a Prototype of Autonomous Decentralized System : An Overview" Proceedings of the 3rd Int'l Symposium on Autonomous Decentralized Systems(ISADS'97), 1997, Pages 85~92.

[5] "Prevalence Tables" Virus Bulletin, January~May 2001, Page 3

[6] http://www.hauri.co.kr

[7] http://www.ahnlab.com