네트워크상에서 바이러스 차단을 위한 실시간 시스템 설계

박상철*, 김원필, 김판구, 이윤배
조선대학교 대학원 전자계산학과
sanchun@mina.chosun.ac.kr

Real-time System Design for Blocking Viruses on the Networks

Sang-Chul Park*, Won-Pil Kim, Pan-Koo Kim, Yun-Bae Lee
Dept. of Computer Science, Chosun University

요 약

PC 통신망 및 인터넷을 통한 새로운 형태의 바이러스가 국내외에 유입되어 빠르게 확산되고 있으며 이에 대한 피해 역시 급증하고 있다. 때문에 새로운 형태의 네트워크 유입 차단용 바이러스 탐지 시스템 개발을 통하여 사전에 네트워크를 통한 바이러스 유입을 방지하고 나아가 그 피해를 최소화 할 필요가 있다. 따라서 본 논문에서는 바이러스 차단에 대한 국내외 기술 현황에 대해 알아보고 기존의 바이러스 차단 모듈에 대해 고찰하고 아울러 네트웍 상에서 바이러스 차단을 위한 새로운 실시간 시스템을 설계하였다.

1. 서론

인터넷 사용의 급증으로 새로운 유형의 바이러스가 국내에 유입되어 빠르게 확산되고 있으며 이에 대한 피해가 엄청나게 커지고 있는 실정이다. 그러나, 현재 사용하고 있는 바이러스 진단 기술은 지금까지 발견된 바이러스에 국한된 진단기술이기 때문에 다양한 플랫폼에서 동작 가능한 새로운 형태의 바이러스들이 계속 발견되고 있는 현실에서는 이에 대한 대비책이 크게 부족하다. 이에 새로운 형태의 네트워크 유입 차단용 바이러스 탐지 시스템 개발을 통하여 사전에 네트워크를 통한 바이러스 유입을 방지하고 나아가 그 피해를 최소화 할 필요가 있다. 미국에서 발생한 97년도 컴퓨터 범죄에 대한 조사에서 바이러스에 의한 피해액이 전체 100 %중 약 12 %를 차지하고 있다. 또한 정보전에서 가장 위협적인 요소로서 등장한 것이 바이러스이기 때문에 앞으로 전개될지 모르는 정보전에 미리 대비하기 위해서는 새로운 형태의 바이러스 차단을 위한 시스템 개발이 필요하다.

본 논문에서는 이러한 필요성에 의해 네트웍 상에서 바이러스 차단을 위한 새로운 실시간 모듈을 설계하였다. 2장 관련연구에서는 국내외 기술 현황에 대해 분석하고 기존의 바이러스 차단 모듈에 대해 알아보며 3장에서는 논문에서 제안한 실시간 모듈을 설계하였으며 4장에서는 결론과 향후 연구과제를 제시하였다.

2. 관련연구

2.1 국외 기술 현황

전세계적으로 매크로 바이러스가 급속히 확산되어 있는 추세이며 인터넷을 통하여 모든 네트워크상에서 발견되고 있다. 알려져 있는 바이러스에 대하여 진단, 치료하는 백신 개발 및 이에 대한 연구를 수행중이며 몇몇 연구기관만이 unknown 바이러스에 대한 연구가 진행 중에 있으며 각종 플랫폼에 적용 가능한 바이러스만을 진단, 치료 가능한 백신 프로그램들이 네트워크 차원에서 등장하고 있다. 그 동안 사용되었던 바이러스 퇴치기술을 보면 다음과 같다.

- 바이러스 감염 위장(infection trickery)
- 알려진 패턴에 대한 검색, 비교방법(Known virus pattern scanning)
- 알려진 패턴을 이용한 모니터링(Monitering)
- 체크섬 및 CRC값 비교(Checksumming & CRC Comparing)

· 인공지능 기법(Heuristic method)

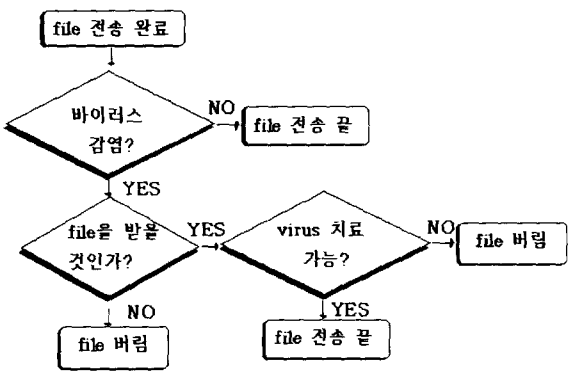
EICAR(European Institute Computer Anti-virus Research:유럽에서 활동중인 민간 바이러스 방지 협회), VB(Virus Bulletin:기술적인 부분을 담당), ICSA(International Computer Security Association:미국의 민간 컴퓨터 보안 협회)등의 민간 차원의 바이러스 기업 및 협회에서 전문가들이 공동으로 새로운 형태의 바이러스 공격에 대한 연구가 계속 진행 중에 있다.

2.2 국내 기술 현황

현재 국내에서는 주로 PC통신을 통해 유포되고 있는 국내 제작 바이러스 및 인터넷을 통하여 유입되는 외국산 바이러스가 주를 이루고 있으며 이들에 대한 진단, 치료 기술로 백신 프로그램을 사용하고 있다. 해당 백신 프로그램은 알려진 바이러스에 대하여 샘플을 입수한 후 이를 분석하여 바이러스가 가지고 있는 진단, 치료에 필요한 특징적 패턴을 추출, 이를 백신 프로그램 내부에 추가하여 진단, 치료에 사용하고 있다. 때문에 새로운 바이러스가 발견되면 이에 대한 대처 능력이 부족하다. 국내 컴퓨터 바이러스 백신 제작 전문업체는 2개 정도이며 나머지 백신 프로그램은 PC통신을 통하여 무료 배포하는 공개 S/W 및 외국산 제품이 있다. 현재는 국내에서 발견된 바이러스에 대해서만 주로 진단, 치료하기 때문에 전세계에서 제작 공급되고 있는 외산 백신 프로그램에 비하여 진단 가능한 바이러스 수가 현저히 적다. 국내의 기술동향으로는 첫 번째, 진단 기술 측면이 있는데 초기 백신이 패턴진단에 의한 방법과 CPU Emulation등이 주류를 이루어 알려진 바이러스와 신고 접수된 바이러스에 대하여 100%진단 치료가 가능하다. 해외에서 Blood Hound, Digital Immune System등 알려지지 않은 바이러스 탐지 기술이 소개 및 연구되고 있으며 국내에서는 하우리에서 알려지지 않은 바이러스 탐지 기술을 적용한 제품을 개발하고 있으며, 두 번째로는 시스템 적용 기술 측면이 있는데 원격 배포, 모니터링 등의 기능 바이러스 분석 서비스와 연계한 바이러스 방역 서비스 개발이 진행 중에 있다.

2.3 기존의 바이러스 차단 모듈

기존의 바이러스 차단 모듈의 가장 기본적인 구조는 방화벽 상에서 패킷을 모니터링을 한 후 모니터링한 패킷을 필터링 함으로써 바이러스를 차단하는 모듈이다. 먼저 네트워크를 모니터링을 하기 위해서는 먼저 네트워크를 통해 지나가는 패킷을 모두 잡을 수 있어야 하고 잡은 패킷들 중에서 미리 입력한 필터의 정보를 참조하여 바이러스 감염 여부를 분석해야 한다. 패킷을 분석하는 모듈은 모니터링 시스템에 따라 수행하는 작업이 달라진다. 만일 패킷 수준의 모니터링 시스템이면 패킷에 들어있는 프로토콜 별로 헤더를 분석하여 사용자에게 정보를 보여줄 것이며 어플리케이션 수준의 모니터링 시스템이면 그러한 패킷들을 모아서 보다 복잡한 정보를 생성한다. 그리고 방화벽에서는 그러한 패킷들에 대해서 각각 특정한 행동을 취한다 즉, 바이러스에 감염되어 있다면 그 패킷을 버릴 것인지 치유할 것인지 그런 일련의 행동을 취하게 된다. 그리고 분석한 패킷이나 모아진 어플리케이션의 정보를 나중에 이용하기 위해서는 적절한 형태로 변형되어 보조 기억 장치로 보내어져서 기록한다. 기존 바이러스 차단 모듈은 아래와 같은 형식으로 구성되어 있다.

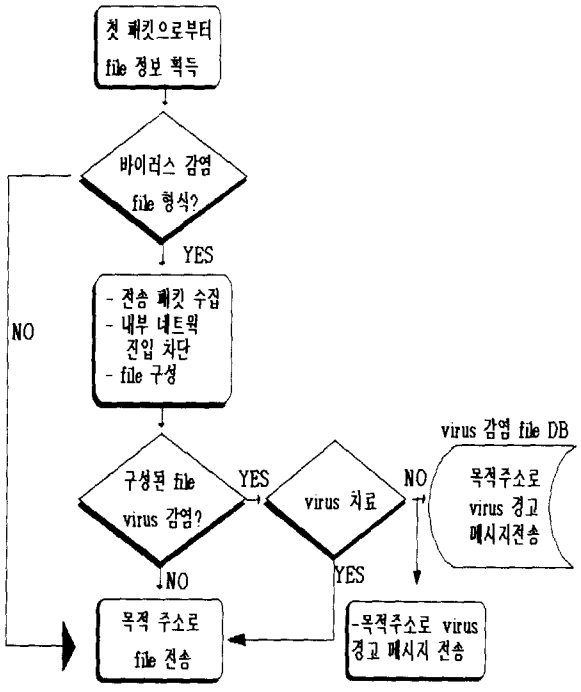


[그림 2.1] 기존 바이러스 차단 모듈 구성도

3. 제안된 실시간 바이러스차단 모듈

모든 패킷은 목적주소에 도달하기 위해서는 해당 내부 네트워크의 게이트웨이를 항상 거치게 되므로, 게이트웨이에서 내부로 들어가는 첫 패킷이 바이러스에 감염될 가능성이 있는 파일 형식이라면 첫 패킷을 내부네트웍으로 들어 갈 수 없도록 차단한다. 첫 패킷을 뺀 나머지 패킷은 목적주소로 모두 보내어진다고 하더라도 첫 패킷을 받지 못하면 완전한 파일을 생성할 수 없으므로 행여 바이러스를 포함한 파일이더라도 위험요소가 없다. 또한 첫 패킷만을 차단하는 이유는 목적주소에서 사용자의 기다림 시간을 최소화하고 모든 패킷을 차단하므로 해서 발생할 수 있는 전체 시스템의 부화를 최소화하기 위함이다. 바이러스 감염 의심이 되는 첫 패킷 이후의 모든 패킷을 수집하여 완전한 파일로 구성하여 바이러스를 체크하고 바이러스가 없다면 목적주소로 보낸다. 그렇지 않고 해당 바이러스 치료가 가능하다면 치료를 하고 목적주소로 보낸다. 바이러스가 치료되지 못한 파일은 바이러스 감염 파일을 모으는 데이터베이스에 출발주소, 목적주소, 파일의 정보 등을 저장하고 목적주소에 파일에 바이러스가 검출되어 치유불가 에러 코드를 보낸다

목적주소에서는 치유불가 에러 코드를 받고 현재 파일 전송되고 있는 파일이 바이러스에 감염됨을 알고 파일 받기를 중단한다. 파일 감염 데이터 베이스에 저장된 파일들은 바이러스 치유프로그램이 처리 할 수 없는 파일들이므로 이를 시스템 관리자에게 알리고, 바이러스 연구 단체에 알려 이 바이러스의 백신을 연구하도록 자료로써 제공되어 질 수 있다.



[그림 3.1] 제안된 시스템 구성도

4. 결론 및 향후 연구과제

본 논문에서는 사전에 네트워크를 통한 바이러스 유입을 방지하고 나아가 그 피해를 최소화할 수 있는 네트웍상에서 바이러스 차단을 위한 실시간 시스템을 설계하였다. 기존 바이러스 차단 모듈은 방화벽이라는 커다란 덩치의 시스템에 의존하여 구성된 모듈이었으며 사용자에게 의지하여 바이러스를 치유하는 방식을 사용하였으나 본 논문에서 제안한 실시간 시스템은 바이러스 차단 전용으로 구성되었으며 사용자에게 의존하지 않은 자체 치유기능과 치유하지 못하는 바이러스에 대해서 데이터베이스를 구성하여 향후 바이러스 연구의 자료로써 역할을 수행할 수 있도록 구성하였다.

향후 연구 과제로는 치유하지 못하는 바이러스에 대해 본 논문에서 제안한 시스템과 목적주소 사용자간에 에러 코드 전송을 통해 바이러스 파일임을 알리는 기능을 추가하여야 한다. 이에 따른 목적주소 파일 전송 프로그램에 이 에러를 처리할 수 있는 코드가 추가되어야 한다.

참 고 문 헌

[1] Dawson R. Engler and M. Frans Kaasheok. DPF: Fast, Flexible, Message Demultiplexing using Dynamic Code Generation. In ACM Communication Architecture, Protocol, and Application (SIGCOMM '96)

[2] Steven McCanne and Van Jacobson . The BSD packet filter: A new architecture for user-level packet filter. In USENIX Technical Conference Proceedings. page 259-269, San Diego, CA, Winter 1993. USENIX

[3] Karanjit Siyan and Chris, "Inter Firewall and Network Security" NRP, 1995

[4] D. Brent Chapman and Elizabeth D.Zwicky, "Build -ing Internet Firewall" O'Reilly & Association, Inc. 1995

[5] William R. Cheswick and Steven M.Bellovin, "Firewall Inter Security" Addison-Wesley, 1994

[6] S.Stolfo, A.Prodromidis, S. Tselepis, W. Lee, JavaAgents for Meta learning over Distributed Databases, in AAAI 97 workshop on AI Methods in Fraud and Risk Management

[7] Neil C.rowe and Sandra Schiavo, An intelligent tutor for Intrusion Detection on Computer System, code Cs/rp, Department of Computer Science, Naval postgraduate school monterey, 1997

[8] http://www.tis.com/ - Trusted Information System

[9] "컴퓨터 바이러스 감염 예방 시스템 개발에 관한 연구", 한국 전산원, 1995