바이러스 면역시스템 분석

한국정보보호진흥원 전 완 근
한서대학교 이 중 식, 이 종 일, 김 홍 윤

요 약

최근에는 러브레터 ,백오리피스와 같은 웜바이러스, 트로이목마, 리눅스바이러스 등과 같은 네트워크 상의 대규모 PC를 대상으로 막대한 피해를 줄 수 있는 악성 신종 바이러스가 출현함에 따라 국내외적으로 증가추세에 있는 신종 바이러스에 대하여 보다 신속하고 능동적으로 대처하기 위해서는 인공지능 기법을 적용한 새로운 형태의 차세대 악성 컴퓨터바이러스에 대한 연구가 요구된다. 이를 위해서 미확인된 차세대 악성 바이러스에 대한 신속한 자동탐지 및 제거기능을 갖는 해외의 디지털 면역시스템을 분석한다.

Analysis of Computer Virus Immune System

(Jeon Wan Keun, Lee Joong Sik, Lee Jong Il, Kim Hong Yoon)

ABSTRACT

To recently with the love-letter and Back Orifice the same Worm-virus, with the Trojan and the Linux-virus back against the new species virus which inside and outside of the country to increase tendency the malignant new species virus which is the possibility of decreasing the damage which is enormous in the object appears and to follow a same network coat large scale PC is being quicker, it disposes spontaneously to respect, applied an artificial intelligence technique the research against the next generation malignant computer virus of new form is demanded. Will reach and to respect it analyzes the digital immunity system of the automatic detection which is quick against the next generation malignant virus which had become unconfirmed and the foreign countries which has an removal function.

1. 서 론

MS-DOS상에서 동작하는 파일, 부트바이러스 등 일반적인 컴퓨터바이러스의 경우에는 감염속도가 느리다. 반면에 1988년 11월에 최초로 등장한 인터넷웜의 경우 인터넷을 통해 사용자의 간섭없이 자동으로 웜을 전파시키는 등 최근의 인터넷기반의 컴퓨터바이러스가 도래하면서 감염속도가 급격히 빨라졌으며 국내에 유입된 미켈란젤로, 멜리사 바이러스, ExploreZip, 러브레터 등과 같은 웜바이러스 경우에서처럼 수시간 또는 수일내에 인터넷을 통해 전세계에 컴퓨터바이러스를 유포되고 있는 실정이다. 이에 대응하는 백신기술은 일정한 개발기간이 소요됨에 따라 대규모적인 컴퓨터바이러스 공격이 이루어질 경우 이에 대한 신속한 대응을 하기에는 아직까지는 어려움이 따르고 있는 실정이었다.

따라서 최근에는 아래와 같이 다양한 요건들이 면역시스템 설계에서 요구되고 있다. 따라서 본 논문에서는 클라이언트-서버 구조로 신종 또는 미확인 바이러스 유형을 탐지· 제거하는 모듈을 액티브 네트워크로 연결된 계층형 구조의 게이트웨이를 통하여 전달함으로서 바이러스를 치료하거나 필요시에 인공지능 기법을 적용하여 차세대 악성바이러스에 대한 탐지 및 제거 모듈인 바이러스 면역시스템에 대하여 분석하고자 한다.

2. 컴퓨터바이러스 감염특성 분석

2.1 개요

수년전에만 해도 플로피디스크 등을 통해 일부 PC들에 컴퓨터바이러스에 감염되어 피해를 주는 정도로 소규모적인 컴퓨터바이러스의 전염성을 갖고 있었다. 그러나 최근에는 네트워크상에 접속된 대량의 컴퓨터에 의존하는 정보화사회가 도래되고 이동코드 형태의 프로그램의 개발과 보급이 확대되면서 E 메일과 인터넷을 통하여 생물학적 바이러스 질병처럼 인터넷기반의 컴퓨터바이러스는 자기자신을 복제하거나 변식하는데 단시간에 감염시킬수 있는 전염성을 갖추게 되었다.

하루만에 수백만대의 PC에 전파력이 강한 컴퓨터바이러스에 감염되어 막대한 피해를 입히는 긴급한 사고가 발생하는데 반하여 이를 치료할 수 있는 백신SW의 개발과 단 하루사이에 백신 업데이트를 위하여 백신업체의 엔진에 대하여 동시다발적으로 다운로드하야 하는 문제점을 야기시킨다. 이는 생물학적인 바이러스의 생성과 소멸을 통한 급속한 질병의 전염성과 같은 컴퓨터바이러스의 특성에 기인한다. 이에 대하여 미국의 Cohen, Murray 등 정보보호 전문가들이 생물학적 바이러스 질병에 대한 전염성에 관한 병리학 이론을 컴퓨터바이러스 대응기술에 적용하는 연구가 진행되어 왔다.

다음은 이와 관련되어 사용되는 주요 전문용어를 정리한 것이다.

- 생성율(Birth rate) : 임의의 바이러스가 하나의 대상에서 다른대상으로 자기복제를 시도하는 비율
- 소멸율(Death rate) : 감염된 대상으로부터 바이러스를 제거하는 비율
- 전염 한계치(Epidemic Threshold) : 바이러스의 생성과 소멸시 연관수치로서 이러한 한계치이상인 경우 집단에 바이러스 감염을 재발하게 되고, 한계치이하인 경우 바이러스가 소멸됨
- 유포(Prevalence) : 임의의 바이러스가 특정한 집단내에 널리 유포되는 정도
- 전염병리학(Epidemiology) : 질병의 전염성에 관한 연구분야
- 감염된 컴퓨터시스템(Infected machine) : 플로피디스켓 또는 다른 컴퓨터로 전달시

킬수 있거나 특정한 컴퓨터바이러스를 보유하고 있는 컴퓨터시스템

- 바이러스 사고(Virus Incident) : 외부단체로 부터 최초로 감염됨에 따라 특정한 바이러스로 인해 임의의 단체 내에 수많은 대상이 감염된 경우
- 사고율(Incident rate): 단위시간당 특정 집단에서 발견된 바이러스 사고발생율

2.2 생물학적 바이러스와 컴퓨터바이러스의 감염특성

일반적으로 생물학적 바이러스(이하 바이러스)와 컴퓨터바이러스(PC 바이러스)는 많은 상이한 전염특징을 갖고 있다.

첫째, 생성율은 개인이 바이러스 감염을 치료하는 빈도수인 바이러스 소멸율에 의존한다. 또한 개인이 질병으로 의심함에 따라 바이러스 감염된 이후에 면역성을 갖추거나 곧바로 바이러스를 타인에게 전염시킬 수 있는 보균자를 갖는데 반하여 PC 바이러스의 생성율은 PC 바이러스 보유자 또는 PC 바이러스의 유포를 조장하는 사람, 프로그램에 PC 바이러스 감염을 위해 사용되는 통신 메커니즘, 컴퓨터시스템간의 데이터 전송율, 플로피디스켓의 쓰기방지 탭 이용 및 백신 프로그램의 활용 등과 같은 사용자의 예방조치 등에 따라 결정된다. 한편 PC 바이러스의 소멸율은 PC 바이러스의 암호화기법을 이용한 은폐와 E 메일 첨부파일 등을 통한 위장하는 특징, PC 사용자의 정보보호 인식과 경계심, 백신 프로그램을 통한 지속적인 PC 바이러스 탐지 및 제거 등에 따라 좌우된다.

둘째, (그림 1)에서 보는 바와 같이 바이러스의 경우 100개 대상의 집단을 모의시험한 결과, 특정한 감염된 대상(Infected machine)이 다른 대상을 곧바로 감염시키거나 해당 바이러스의 생성율은 소멸율에 비해 5배에 이르렀다. 이는 면역성이 없는 대상은 해당 바이러스를 치료했음에도 불구하고 바이러스 보균자의 타인과 접촉을 통해 단기간에 지속적인 바이러스의 감염이 진행된 결과이다. 따라서 단체의 전염한계치에 따라 결정적으로 급격히 바이러스가 번식되거나 소멸하게 된다.

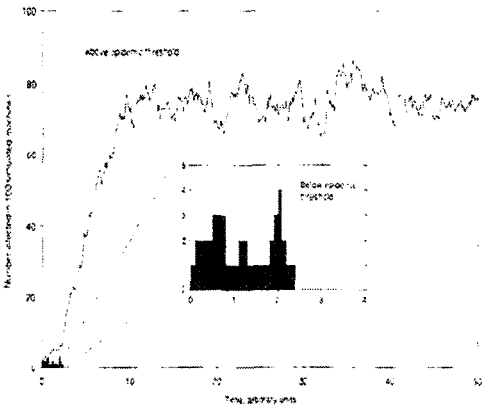

그림 1 바이러스 전염한계치

이에 반하여 (그림 2)에서 보는 바와 같이 PC 바이러스의 경우 정보보호 인식이 잘된 500개 업체를 대상으로 1,500여개의 서로다른 PC 바이러스 샘플을 통해 모의시험한 결과, 15%이하의 PC 바이러스 감염사고율을 나타내었고 이러한 감염사고율은 단한번에 나타나지도 않았다. 이는 1,500개의 PC 바이러스 샘플에 대한 전염한계치가 낮았으며 다량의 PC 바이러스 감염이 이루어지지 않은 결과이다. 따라서 PC 바이러스에 대한 전염한계치를 낮추게 되면 추후에 동일한 PC 바이러스가 출현되더라도 해당 PC바이러스로 인한 커다란 피해규모를 줄일 수 있다. 그러나 일부 사용자가 임의의 PC 바이러스를 제거했다 하더라도 다른종류의 신종 PC 바이러스가 등장하여 이에 대한 치료를 할 수 있는 백신 프로그램이 개발되기 이전까지는 해당 PC 바이러스에 대한 전염한계치는 여전히 높아질 수 밖에 없게 된다. 그러므로 대국민 대

상 PC 바이러스 예방 및 대응관련 홍보물 제작·보급을 통한 정보보호 인식 확산과 함께 지속적인 신종 PC 바이러스에 대한 백신프로그램 개발 및 보급이 무엇보다도 중요하다고 하겠다.

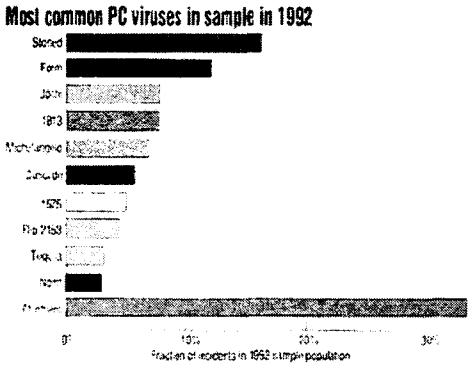

그림 2 PC 바이러스 전염한계치

3. 국외의 디지털 면역시스템 분석

3.1 개요

대부분의 파일, 부트 바이러스 등 전형적인 컴퓨터바이러스의 감염속도가 더딘 반면에 1988년 11월에 최초로 등장한 인터넷웜의 경우, 인터넷을 통해 사용자 간섭없이 자동으로 웜을 전파시키는 등 최근의 인터넷기반의 컴퓨터바이러스가 도래하면서 감염속도가 급격히 빨라졌으며 미켈란제로·멜리사 바이러스, ExploreZip 등의 인터넷웜 등의 최신 바이러스 추세는 수시간 또는 수일내에 인터넷을 통해 전세계에 컴퓨터바이러스를 전파되고 있다.

이에 따라 컴퓨터바이러스 전파속도 보다 신속한 치료법 제공, 신종 또는 알려지지 않은 컴퓨터바이러스 자동탐지, 전염성 및 바이러스 쇄도에 대응하는 처리기술, 자동으로 바이러스 치료를 위한 신속한 처리속도, 급변하는 위협에 신속히 대응할 수 있는 유연성, 백신기술의 안전성 및 신뢰성 보장, 기관의 보안정책에 일치하는 사용자 보호정책 유지기능 등 다양한 바이러스 백신기술이 요구되고 있다. 최근 단시간에 급속도로 전파되는 인터넷기반의 컴퓨터바이러스가 급증하는데 반하여 백신기술은 일정한 개발기간이 소요됨에 따라 대규모적인 컴퓨터바이러스 공격이 이루어질 경우 이에 대한 신속한 대응을 하기에 어려움이 따른다. 이에 착안하여 액티브 네트워크상에서 자동으로 백신기능을 개발·보급해주는 차세대 백신기술인 컴퓨터바이러스 디지틀 면역시스템에 관한 연구가 미국 등 선진국을 중심으로 활발히 진행되고 있으며, 이미 상용화된 상태이다. 이와 관련하여 최근에 시만텍과 IBM에서 공동으로 개발한 디지털 면역시스템를 분석하여 보면서 디지털 면역시스템의 구성요소와 구성요소들의 각각의 기능과 필요로 하는 네트워크의 프로토콜등을 살펴본다.

3.2 시스템 구조 및 기능 분석

o 시스템 구조

로컬네트워크의 클라이트에서 발견된 신종바이러스 혹은 미지의 바이러스와 같이 악성 바이러스의 전파 속도보다 더 빠르게 치료하기 위해, 바이러스의 샘플이 발견되는 즉시 관리시스템(면역시스템관리자)에 의하여 판단하여, 로컬 혹은 바이러스 분석 센터를 통하여 샘플에 대한 분석과 치료 및 제거 모듈을 개발하여 감염된 시스템이나 미연의 방지를 위한 네트워크에 다시 보내어 질 수 있도록 게이트웨이로 연결되어 액티브네트워크와 (그림 3)과 같이 계층적인 구조로 되어있다.

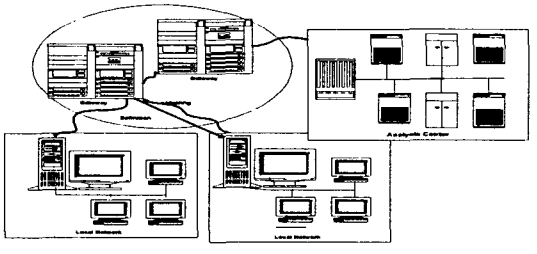

그림 3 디지털 면역시스템 구조

o 시스템의 기능

- 컴퓨터바이러스 탐지기능 : 바이러스에 감염된 파일이나프로그램 실행이 되기전에 미리 발견할 수 있어야하고 그에 따른 후속대응책을 만들 수 가 있다. 이에따라 디지털 면역 시스템에서는 각각의 클라이언트시스템에 설치된 안티바이러스 제품에 의해서 가지고 있는 바이러스들에 대한 문자열 패턴매칭을 통하여 바이러스가 발견이 가능하다. 그러나 발견된 바이러스에 대한 구체적인 정보가 없을 경우에는 신종인지 혹은 미지의 바이러스가 전혀 알려져 있지 않은 바이러스인지를 구분을 할 수 없는 상태이다. 이에 따라서, 바이러스프로그램이나, 감염된 시스템의 작동상태, 바이러스가 실행되었을 때 시스템의 상태을 알기위해 시뮬레이션 기법과 디버깅기법등의 다양한 분석 방법을 통하여 어느 정도 유추하여 낼 수가 있다. 유추된 샘플을 변형이 없이 로컬 안티바이러스 관리자(시스템 관리자)에게 발송한다.
- 관리자 시스템 : 샘플을 처리하기 위해 시스템관리자 혹은 방역 시스템과 같은 관리자 시스템을 두어 제시된 샘플을 즉각 처리할 수 있도록 가장 최근의 업데이트된 컴퓨터바이러스 정의에 의하여 샘플을 제출한 클라이언트에게 즉각적으로 해결책을 보내질 수 있도록 작동한다. 또한, 관리자 시스템에서는 조직의 내부 네트워크가 면역시스템을 반드시 경유하여 출입하도록 할수있으며, 하나 또는 그 이상의 모아진 샘플에 대한 관리와 긴급한 샘플에 대해서 요구하기 우선순의적 처리를 위해서 시스템의 설정 등을 바꿀 수 있다. 모든 샘플들은 큐상에서 관리가 되며 순차적인 번호에 의해서 관리가 되지만 여러 경우에 의해서 우선순위가 바뀔 수 가 있다.
- 컴퓨터바이러스 분석기능 : 관리자시스템을 거쳐 온 바이러스 샘플을 가장 중요한 구성요소인 바이러스 분석센터에선 분석하여 바이러스 정의를 업데이트하고 그 치료방법을 패키지화하고, 그것을 클라이언트에게 자동으로 분배된다.
- 치료모듈 분배기능 : 바이러스 분석 센터에서는 주어진 샘플에 대한 분석하는 기능과 함께 분석된 정보를 정의 업데이트하고 치료방법을 만들고 다른 네트워상의 사용자들 보호하기 위해 그 업데이트 정보를 최초로 바이러스에 감염이 된 것을 보고한 클라이언트로 돌려준다.

3.3 컴퓨터바이러스 자동분석센터

o 시스템의 구성

액티브네트워크를 통하여 시스템관리자(면역시스템관리자)에게 전달된 샘플을 안전하게 분석 및 관리를 위하여 (그림 4)와 같이 방화벽을 두었으며 바이러스 샘플의 분석과정에서 필요로 하는 컴퓨터 시트템이나 자원설정 등과 분석자료에 대한 의사결정과 예외적인 바이러스의 취급을 위한 판단이 수퍼바이져를 통하여 이루어진다.

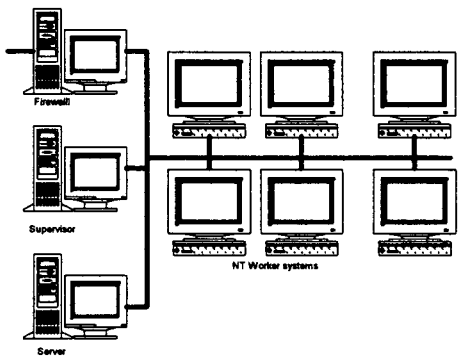

그림 4 컴퓨터바이러스 자동분석센터

또한, 바이러스의 분석에 쓰일 워크시스템을 NT머신과 IBM계열의 컴퓨터로 나뉘어져있어 경우에 따라서 조합하여 사용할 수 있도록 하였다. 바이러스를 포함하고 있는 샘플을 분석해서 그 바이러스를 탐지하고 처리할 수 있는 바이러스의 최신 정보와 정의파일을 모든 바이러스 샘플들에게 적용될 수 있는 지 확인하기 위해서 테스트를 거쳐, 일단 테스트를 완료하게 되면 바이러스 정의파일은 바이러스 샘플을 제출하였던 모든 조직들로 액티브네트워크을 경유해서 보내도록 한다. 그리고 샘플을 분석과정에서 생성되는 정의 파일이나 정보들은 서버에 저장이 된다.

o 분석과정

컴퓨터바이러스 분석센터는 입수된 샘플이 감염이 되었을 경우에는 어떠한 형태의 바이러스인지를 결정하고 분석하기 위하여 여러 단계의 처리 과정을 거치게 되는데 바이러스이 형태가 분류된 형태에 같은 종류의 형태가 있다면 신뢰할 만한 분석을 위해서 바이러스의 샘플을 얻을 수 있도록 충분한 횟수를 거쳐서 복제시킨다. 복제된 바이러스를 바이러스의 탐지 및 검증을 위하여 분석하면서 나오는 추출된 정보들은 바이러스의 정의을 결정하는데 사용되며 만들어진 바이러스의 샘플들에 대해서 시험을 통하여 일반적인 바이러스의 정의 값을 가지게 되고, 최종적으로 업데이트된 정보를 시스템이나 사용자에게 돌려주게 된다. 이와 같은 모든 과정은 독립적으로 모듈별로 이루어지며 각 과정에서 수퍼바이저는 각 샘플 분석 단계에서 수행될부분이 무엇인지, 작업이 수행될 때 필요한 시스템은 어떤 것인지 알고있다. 이 무엇인지, 작업이 수행될 때 필요한 자원이 어떤 것인지 알아야 한다.

(그림 5)와 같이 여러 단계를 통하여 이러한 작업이 자동으로 이루어지게 된다.

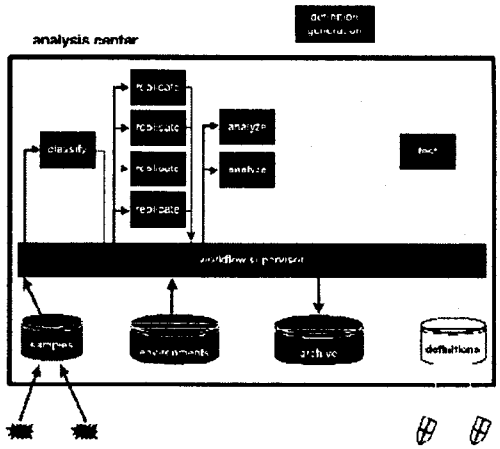

그림 5 컴퓨터바이러스분석센터 업무흐름도

- (1단계) 분류화과정(Classification) : 분류화과정에서는 입수된 바이러스의 샘플 타입을 분류하는 과정이다. 예를 들어 도스형바이러스(COM,EXE) 아니면 마이크로 소프트워드 파일을 감염시키는 바이러스인지 등을 결정한다.
- (2단계) 환경조성 (Creation of the replication environment) : 환경조성단계에서는 각각의 바이러스의 샘플 유형(DOS/윈도우95/98형 바이러스, 윈도우NT형인지 리눅스바이러스, 매크로바이러스) 맞는 적합한 복제 환경이 선택되어지면 그 환경의 이미지를 서버에서부터 획득하고 한 대 또는 여러 대의 적절한 타입의 워크시스템을 수퍼바이져가 선택을 하여 설치된다.
- (3단계) 감염과정 (Replication) : 신뢰성있는 분석을 할 수 있도록 바이러스 샘플을 충분하게 획득할 수가 있도록 조성된 ted 환경에서 한 대혹은 여러대의 바이러스를 감염을 동시에 실행한다.
- (4단계) 분석과정 (Analysis) : 컴퓨터 바이

러스 분석단계에서는 특징적인 문자열을 추출하고, 분석된 바이러스에 대한 모든 정보를 각각의 형식에 맞게 따라 맵핑한다.

- (5단계) 정의생성 (Definition generation) : 바이러스의 분석단계를 거치면서 자동 혹은 수동으로 정의를 생성할 수 있도록 하였으며, 언제나 바이러스 분석 매뉴얼의 결과에 따라 바이러스 정의를 업데이트 할 수 있도록 하였다. 정의되는 바이러스는 순차적인 번호로 관리를 한다. 정의사이에 일치성을 보장하기 위해서 단일 정의 시스템을 사용한다.
- (6단계) 테스트단계 (Test) : 하나의 업데이트된 정의파일이 사용가능하다면 그 정의된 파일이 어떤 파일에든 적절히 탐지됨을 검증하기 위한 테스트과정을 두고, 모든 파일에 대해서 적용이 되고 모든 파일을 치료 할 수 있다면 그 정보값은 수퍼바이저 시스템에 의해 샘플을 제출한 바이러스를 해결책으로 제공되기위해서 액티브네트워크로 보낸다.

위와 같은 6단계의 과정을 거치면서도 샘플이 전혀 새롭고 복합적인 타입의 바이러스를 포함하고 있을 경우와 같이 분석센터에서 직접 관리할 수 없다고 판단이 내려지면 분류화, 감염, 분석, 테스트의 결괴등을 포함한 정보와 함께 분석가에게 관리된다. 또한, 바이러스의 정의는 발표되기 전에 엄격히 테스트와 최종적으로 분석이 이루어지는 어떠한 과정에서 문제점과 맞닿게 될 경우에도 수동으로 관리할 수 있도록 분서가에게 이관되도록 한다.

3.4 액티브 네트워크

디지털 면역 시스템에서 사용된 액티브네트워크는 (그림 6)와 같이 게이트웨이라고 불리는 node로 루트와 가지로 이루어진 트리모양으로 구성하였다.

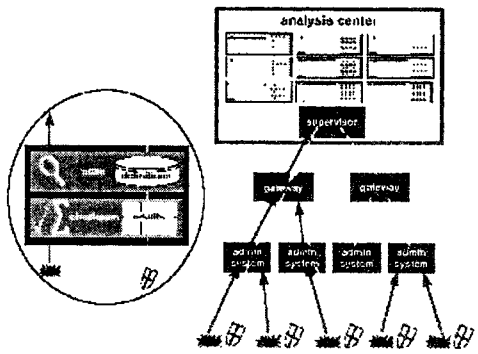

그림 6 액티브 네트워크

트리에 있어서 루트는 바이러스 분석 센터이고 트리의 가지부분은 개개의 관리자시스템에서, 샘플 그리고 업데이트된 바이러스의 정의 및 치료모듈이 전달된다. 관리자시스템들에게 필요에 따라 적절하게 어드레스해서 전송가능하도록 한다.

- 액티브 네트워크 게이트웨이 : 디지털 면역 시스템에서 사용된 액티브네트워크는 node로 루트와 가지로 이루어진 트리모양으로 구성된 게이트웨이의 두 가지 중요한 기능을 하는 데 그중 하나는 체크섬의 기능으로 바이러스의 감염여부를 판가름하거나 상위의 네트워크를 지나는 지의 여부를 나타내는 데 쓰인다. 게이트웨이의 두 번째 기능은 샘플파일을 가장 최근의 바이러스 정의로 스캔하고, 만약에 바이러스의 샘플이 수분 전에 바이러스 분석센터에 의해서 분석이 되었을 지라도, 긴급한 바이러스일 경우에는 액티브 네트워크에 의해서 빠르게 관리되어지도록 한다.
- 액티브 네트워크 프로토콜 : 안전성과 신뢰성있는 액티브 네트워크를 설계를 위해서는 학습형 바이러스의 면역 시스템은 신뢰

성이 있어야 하며, 특히 민감한 정보가 폭로 또는 위조된 바이러스 정의 파일등의 배달이 되지 않도록 보호되어야만 한다. 따라서, 샘플을 분석센터나 게이트웨이에 전달이 되는 과정에서 상호인증하는 과정을 절차를 두어 신뢰성을 충족시키게 하였고, 바이러스의 샘플과 그 바이러스의 정의 파일과 정보들은 반드시 암호화되도록 하여 보안성을 갖추도록 하였다.

바이러스면역시스템(AVIS :AntiVirus Immunity System)의 네트워크 프로토콜 구조는 (그림 7)에서와 같이 계층형 방식의 액티브 네트워크로 구성하여 IP(패킷처리) → TCP(세션처리) → SSL(보안기능처리) → HTTP(클라이언트-서버 기능처리)→AVIS(다중 트랜잭션 처리)과 같은 흐름을 거치도록 하였다.

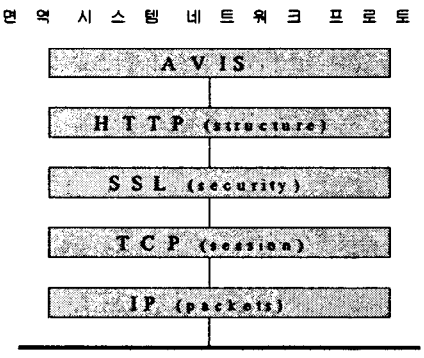

그림 7 액티브 네트워크 프로토콜

4. 결 론

최근에 국내외적으로 활동중인 컴퓨터바이러스는 대부분 E 메일을 통하여 전파되는 인터넷 웜과 매크로바이러스 및 트로이목마가 주종을 이루고 있다. 이는 지금 현재에 주로 사용되는 윈도우시스템 환경에서의 PC를 대상으로 제작된 경우이나, 올해 초에서부터 해외에서 발생한 컴퓨터바이러스 중에는 향후 리눅스기반의 PC 서버를 겨냥하여 제작되는 리눅스 바이러스와 진보된 형태의 해킹기법과 결합된 신종 컴퓨터 바이러스가 주종을 이루리라 예측된다.

이에 따라 컴퓨터바이러스·인터넷웜·트로이목마 등 악성 프로그램 방지지침 개발과 리눅스 바이러스 기법 및 대응기술 연구, 해킹기법 응용 트로이목마 탐지 및 제거기술 연구, 차세대 악성 컴퓨터바이러스 시험분석 연구 등의 컴퓨터바이러스 대응관리시스템 개발과 더불어 국내 백신업체·관련학계 전문가와 공동으로 차세대 악성 컴퓨터바이러스 대응을 위한 학습형 면역시스템 연구과제를 수행하여 향후에 기승을 부릴 컴퓨터바이러스 대응을 위한 기반기술에 대한 연구가 필요하다.

참고문헌

[1] Steve R. White and Morton Swimmer, Edward J Pring, William C Arnold, David M Chess & John F Morar "Anatomy of a commercial-grade immune system", The 9th International Virus Bulletin Conference and Exhibition, Vancouber, 30 September -1 October, 1999. http://www.av.ibm.com/PapersFrame/papersframe.html

[2] The Michelangelo virus http://www.symantec.com/avcenter/-venc/data/stoned.michelangelo.html

[3] Melissa virus http://www.symantec.com/avcenter/-venc/data/mailissa.html

[4] Steve R. White, Jeffrey O. Kephart, and David M. Chess, "The Changing Ecology of Computer Viruses", Proceedings of the

Sixth International Virus Bulletin Conference, Brighton, UK, 1996, pp. 189-202.

[5] CERT Advisory, http://www.cert.org/advisories/C-A-99-04-Melissa-Macro-Virus.html

[6] A description of the ExploreZip worm can be found on the Web at: http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html

[7] U.S. Patent 5,485,575, David M. Chess, Jeffrey O. Kephart, and Gregory B. Sorkin, "Automatic Analysis of a Computer Virus Structure and Means of Attachment to its Hosts".

[8] 한국정보보호센터, "'99해킹·바이러스 현황 및 대응", 1999.

[9] 정보보호21, 김재성 "컴퓨터바이러스 감염특성에 관한 고찰", 2000. 3

[10] 한국정보보호센터, http://www.certcc.or.kr/paper/papers_certcckr.html

전 완 근

1998년 한서대학교 전산정보학과(이학사)

2000년 한서대학교 전산학과(이학석사)

2000 ~ 현재 한국정보보호진흥원 연구원

관심분야 : 컴퓨터 바이러스, 해킹, 인터넷 라우팅

E-mail : wkjeon@kisa.or.kr

이 중 식

2000년 한서대학교 컴퓨터과학과(이학사)

2002년 한서대학교 정보보호공학과(공학석사)

2002년 ~ 현재 한서대학교 시간강사

관심분야 : 컴퓨터 바이러스, 네트워크 보안

E-mail : jslee@hanseo.ac.kr

이 종 일

2000년 한서대학교 물리학과(이학사)

2002년 한서대학교 정보보호공학과(공학석사)

2002년 ~ 현재 한서대학교 시간강사

관심분야 : 정보보호, 무선 인터넷 보안

E-mail : jepplee@hanseo.ac.kr

김 홍 윤

1982년 인하대학교 전자계산학과(학사)

1984년 인하대학교 전자계산학과(석사)

1996년 인하대학교 전자계산학과(박사)

1995년 ~ 현재 한서대학교 컴퓨터통신공학과 부교수

관심분야 : 인터넷 라우팅, 컴퓨터 바이러스, 인터넷 보안

E-mail : hykim@hanseo.ac.kr