서울여대 보안 동아리 스윙에 관한 소개와 연구활동

김미애*

Introduction SWING(Seoul Women's University Internet & Security Group) and Research Activities

Mi-ae Kim

요 약

서울여대 인터넷 보안 그룹인 스윙에 대해 소개하고, 현재 진행중인 연구활동에 대한 간략한 소개와 그 중 안티바이러스 연구에 대해 좀 더 구체적으로 설명하도록 하겠다. 안티바이러스 연구의 내용 중 바이러스 감염 경로, 진단 방법, 기존 안티바이러스 엔진 동작, 연구 수행 활동과 앞으로의 연구 방향에 대해서 다루도록 하겠다.

ABSTRACT

Intoduction SWING and progress of research activities. Then I will explain about Anti-Virus research, concretely. It will deal with Computer Virus infection route, Computer Virus diagnostic methods, exsisting Anti-Virus Engine operation principle, performming research activitis and future research course.

Ⅰ. 서 론

전국 주요대학에서 활동중인 해킹·바이러스 등 정보보호 관련 동아리가 건전한 방향으로 활성화 되도록 지원하여 향후 국가의 주요 정보기반을 보호하고 산업현장에서 활동할 수 있는 정보보호 전문가 육성을 위한 한국 정보보호 진흥원 주관의 2003년 대학 동아리 정보보호활동 지원사업의 일원인 서울여대 인터넷 보안 그룹 스윙에 대한 간략한 소개와 운영방법, 관심분야 및 현재 진행중인 연구 활동에 관한 소개와 그 중 Anti-Virus관련 프로젝트에 관해 좀 더 상세히 기술하도록 하겠다.

Ⅱ. 서울여대 스윙 소개

1. 연혁 및 구성

스윙(SWING)은 서울여대 인터넷 및 보안 그룹의 약어로 1996년 3월에 설립되었다. 서울여대 정보통신대학 부교수로 재직중인 김명주 교수님을 지도교수님으로 하여 현재 10기(2학년) 22명, 9기(3학년) 7명, 8기(4학년 및 7기 중 복학생) 20명, 대학원생(석사·박사) 5명, 모두 52명의 인원이 활동

* 서울여대 보안 동아리 스윙7기 김미애(ntn0001@swu.ac.kr)

중이다. 그리고 4학년 이혜진 학생이 한국 정보보호 진흥원이 지원하는 대학 동아리 정보보호 활동인 KUCIS의 중부권역 회장을 맡고 있다.

2. 운영 방법

스윙은 서울여대 컴퓨터 학과의 ISP(Internet Security & Parallel processing Systems)연구실을 중심으로 운영되고 있다. 현재 1명의 박사과정 대학원생과 5명의 석사과정 대학원생이 있다. 석사 1학기 대학원생들을 주축으로 각 기수들을 맡아 지도하고 있다.

4학년 학생들의 경우 관심 연구 활동에 따라 소그룹을 만들어 각 그룹별 매주 세미나 및 관련 활동을 하고 있으며, 한 달에 두어 번에 걸친 전체 소그룹 모임을 통해 진행 과정에 관한 발표 및 개선 사항에 대한 토론의 시간을 갖고 있다. 그 외 2학년과 3학년 학생들의 경우 각 기수별로 관심 있는 분야를 선택해 자체 세미나를 학기 중에는 일주일에 한 번 정도, 방학 중에는 일주일에 두 세 번 정도 가지며, 각 기수를 담당하는 석사과정 대학원생들의 지도를 받게 된다. 또한 소그룹 및 기수별 활동 외에도 스윙 춘·추계 인터넷 보안 포럼을 개최해 졸업 생 및 자매결연 업체의 인력을 초빙해 강연을 듣는 기회도 마련하고 있으며, 정보보안 관련 학회 세미나 참석 등 많은 활동을 하고 있다.

그리고 위에서 기술한 스윙 자체 내의 학술 활동 외에도 교내 부서와 부설 기관의 바이러스 및 시스템 점검, 타과 및 정보통신 신입생들을 위한 컴퓨터 교육, 지역 주민을 대상으로 하는 컴퓨터 교육, Cyber118활동 지원 등 교내외 봉사 활동도 이루어지고 있다.

여기에 더해서 KUCIS(Korea University Clubs of Information Security)홈페이지 구축 및 관리활동을 병행하고 있다.

3. 관심 분야

정보보안 관련 동아리인 만큼 주요 관심 분야는 당연히 보안 분야이다. 주로 SecureOS나 서버 보안 도구 운영 및 시스템 취약성 분석과 같은 시스템 보안 분야, N-IDS를 연구하고 개발하는 네트워크 보안 분야, 컴퓨터 바이러스 관련 분야 등이 이에 해당한다.

그리고 이런 전문적인 보안 분야를 연구하기 위해 기본적인 보안 점검 및 교육도 이루어지고 있다. 예를들어 Unix, Linux와 같은 운영체제에 대한 기본적인 교육, C/C++/JAVA 프로그래밍, 보안 이해·활용을 위한 지침 및 관리 능력에 관한 교육 등을 하고 있다.

현재 4학년을 중심으로 하는 소그룹의 경우 처음에 설명한 좀 더 구체적이고 전문적인 보안 관련 연구활동이 이루어지고 있다. Procmail source 설치 및 분석, Snort source 설치 및 분석 등이 그 예이다. 그리고 2학년의 경우 Unix와 C 프로그래밍에 관한 세미나를 자체적으로 매주 모임을 통해 주최하고 있으며, 3학년은 Linux에 관한 기본 지식 습득 및 서버 설치에 관한 것을 먼저 익힌 후 현재, Linux해킹 분야에 대한 세미나를 자체적으로 하고 있다.

이 외에도 KUCIS 활동으로 중부권역 세미나를 올해 3월에 서울여대에서 개최하였고, 매 달 중부권역에 속한 다른 학교에서 열리는 세미나에도 참석하고 있다.

Ⅲ. 진행 중인 연구활동

1. UNIX 서버 보안 관련 연구

인터넷 서버의 주종인 유닉스 서버에 대한 관리 교육이 필요성에도 불구하고 매우 미흡한 상태이다. 현재 가장 보편적인 교육방법이 대학이나 전문 교육기관에서 개설된 "유닉스 운영체제" 과목을 통한 것이며, 고가의 유닉스 서버 구입 시 이루어지는 1~2주 기간의 고객 상대 교육이 그나마 이를 보안해 주는 실정이다. 게다가 이런 유닉스 교육은 일반 사용자 교육 중심이므로, 시스템 관리자를 위한 내용은 상대적으로 극히 빈곤하며, "정보보안" 측면에서의 유닉스 서버 관리교육은 거의 전무한 형편이다. 따라서 유닉스 서버에 대한 관리 기법을 "정보보안 "측면에서 다시 정립, 이를 디지털 컨텐츠로 제작하여 보급하는 것이 이 연구의 목적이라고 볼 수 있다.

현재, 관련 강의록을 제작 중에 있으며, 지금까지 구축된 디지털 컨텐츠는 웹사이트를 통해 공개하고 있다.

2. 메일 서버 스캐너 관련 연구

정보 기술의 고속 성장과 초고속 통신망의 발달로 인해 인터넷 사용자 수는 기하급수적으로 늘어나고 있으며, 그에 따라 인터넷을 이용한 다양한 서비스가 이용되고 있다. 그중 E-mail은 인터넷 이용자라면 누구나 사용하는 서비스라고 할 수 있을 만큼 우리 생활의 일부분을 차지하고 있다는 것이 사실이다. 그러나 자신의 메일함은 대부분이 본인의 동의도 얻지 않은 스팸메일로 가득 차있기가 일쑤이다. E-mail 서비스 제공 사이트에서는 스팸메일을 걸러주는 서비스를 대부분 적용하고 있지만, 여전히 스팸메일에서 자유로워질 수 없다. 이러한 스팸메일의 내용은 대부분이 음란물이나 성인사이트로 이를 받는 이가 초등학생이나 중·고등 학생일 경우 교육적인 면에서도 상당히 좋지 못하다. 이 외에도 개인정보 유출에 대한 불안감을 가중시키는 등 스팸메일은 인터넷 사용자에게 많은 피해를 주고 있다.

따라서 이 연구에서는 SMTP(Simple Mail Transfer Protocol)을 이용하여 전송되는 메일을 대상으로 스캔하여 메일박스로 이동되기 전에 스팸메일 및 악성코드 감염메일 등을 검사하여 그에 따른 적절한 대응을 하는 것이 목적이다.

현재 메일 메시지의 헤더와 본문에서 특정 정보를 찾아 정의된 규칙에 따라 적절한 조치를 수행하는 프로그램으로 외부에서 sendmail을 통해 들어오는 메일을 MDA 수준에서 필터링할 때 주로 사용되는 Procmail을 Unix 서버에 설치하여 작동 원리를 이해하고, 내부 소스를 분석하는 중이다.

3. Anti-Virus 관련 연구

컴퓨터 바이러스란 사용자 몰래 다른 프로그램에 자기 자신을 복제하는 명령어를 가지는 프로그램을 말한다.[1] 최근 인터넷의 대중화로 E-mail 사용이 급증하게 되었으며, 클라이언트의 컴퓨터는 대부분 윈도우즈 운영체제를 사용하게 되었다. 이것은 네트워크가 컴퓨터 바이러스의 감염 매체이고, 윈도우즈 환경의 취약점과 MAPI(Messaging Application Program Interface)는 바이러스 제작자들에게 다양한 악성 프로그램을 쉽게 만들 수 있는 환경을 제공하였다.[2]

E-mail로 확산된 웜(Worm)의 등장은 악성 프로그램으로 인한 대규모 피해를 예고하였고, 그것의 예로 Win32/Nimda는 IIS 웹서버의 취약점을 이용한 것으로 E-mail에 첨부된 readme.exe를 실행시키지 않고 읽기만 한 상태로 감염된다. 또한 읽기/쓰기가 가능하도록 공유된 컴퓨터의 경우 네트워크를 통해서도 전파되어 제2차, 제3차의 피해로 확산될 수 있다. 그리고 얼마 전 전세계의 인터넷을 마비시키는 큰 피해를 안겨준 MS SQL 웜 Spida의 경우만 보아도 이제는 바이러스를 그냥 간과할 수 없으며, 안티바이러스(Anti-Virus)분야는 빼놓을 수 없는 중요한 보안 시스템이라는 것을 알 수 있다.

따라서 스윙에서는 현재 안티바이러스 연구를 위해 여러 가지 바이러스 샘플 수집 및 바이러스 특성 연구, 안티바이러스 엔진 3종 벤치마킹,공개 안티바이러스 엔진 소스 분석 등이 이루어지고 있다.

바이러스 감염경로, 바이러스 진단 방법, 기존 안티바이러스 동작원리 등에 대해 알아보고, 위에서 기술한 안티바이러스 연구 활동으로 진행했던 안티바이러스 엔진 3종 벤치마킹 및 관련 활동 사항에 대한 간략한 소개와 향후 연구 방향에 대해 설명하겠다.

3.1 바이러스 감염 경로

바이러스의 감염경로는 여러 가지가 있는데 그중 첫 번째는 저장매체를 통한 감염이다. 저장매체에는 플로피 디스크, CD, 그 외의 휴대용 하드디스크, 스마트 미디어 카드(Smart media Card), MMC (Multimedia Card), 메모리 스틱 등이 있다. 특히 CD의 경우 자동 실행을 위한 AUTORUN.EXE파일이 바이러스에 감염될 경우 CD를 CD-ROM에 넣는 순간 자동으로 바이러스가 실행될 수 있다.

두 번째는 다운로드를 통한 감염으로 공개자료실, FTP, 뉴스그룹, IRC, 메신저, P2P를 통한 감염이 이에 해당한다. 공개자료실이나 FTP를 통해 바이러스에 감염된 파일을 다운로드 받게될 경우 바이러스에 감염되게 된다. 그리고 메신저를 통한 감염의 예로 2002년 2월 14일엔 인터넷 익스플로어의 취약성을 이용해 MSN 메신저로 특정 주소를 모든 사람에게 보내는 JS/Exploit.Messenger웜이 발견되었다.[3]

세 번째는 전자메일과 공유폴더를 통한 감염으로 최근 들어 악성코드의 감염경로로 가장 많이 악용되는 매체로 이들의 안전한 사용이 중요하다. 전자메일의 경우 메일 제목이나 내용으로 메일 수신자를 유혹하거나, 주로 아웃룩 익스프레스에서 메일을 열

어보거나 미리 보기만 해도 감염되는 웜이 발견되기도 했다. 공유폴더의 경우는 특정 폴더를 여러 사람들이 함께 사용할 수 있어 편리한 기능이지만 그만큼 바이러스의 주요목표가 되고, 연결된 다른 컴퓨터에 침투하기 쉽다.

마지막으로, 보안 취약성을 이용해 감염시키는 경우가 있다. 이 경우 웹브라우저의 취약성을 이용해 사이트에 방문하는 것만으로도 상대방 컴퓨터의 시스템에 접근할 수 있고, 님다 바이러스(Win32/Nimda Virus)는 취약성이 존재하는 IIS 웹 서버를 감염 시켜 해당 웹 서버에 접속하는 사용자가 쉽게 바이러스에 감염되도록 한다.[3]

3.2 바이러스 진단 방법

여러 가지 경로를 통해 바이러스에 감염었을 때, 진단하기 위한 방법으로는 첫째, 기본 진단법이 있고, 두 번째, 응용 진단법이 있다. 우선 기본 진단법에는 바이러스가 가지는 고유한 문자열(Signature)을 추출하여 감염 여부를 진단하는 방법으로 초기부터 지금까지 널리 사용되는 방법이지만 바이러스 수가 늘어나면 관리가 복잡해진다는 단점이 있다. 기본 진단법에 또다른 방법으로는 코드 전수 검사법이 있는데, 바이러스가 변형 가능한 모든 형태의 코드 구성을 파악하여 검사하거나 바이러스가 만들어내는 모든 코드의 조합을 검사하는 방법으로 다형성 바이러스 검사에 주로 활용된다.[3] 그러나 변형 바이러스 진단에 유용한 반면, 바이러스마다 각각 검사법을 만들어야 하므로 구성이 복잡하고, 검사 시 모든 코드의 구성확인을 위해서는 많은 시간이 소요된다.

응용진단법에는 서명 검증법, 휴리스틱(Heuristic)검사법, 바이러스 가상 실행법, 특정 위치 진단법 등이 있는데, 이 중 특정 위치 진단법에 대해 알아보면, 1991년 안철수 박사에 의해 고안되어 국내에 소개된 기법으로 크게 프로그램 실행 시작점(Entry Point)으로부터 일정한 거리에 위치한 진단 문자열을 검사하는 방법, 전체 크기를 기준으로 앞이나 뒤로부터 일정한 거리에 위치한 부분을 진단하는 방법 두 가지로 나뉜다.

3.3 기존 안티 바이러스 동작 원리

안티바이러스 동작은 예방용 프로그램, 진단용 프로그램, 치료용 프로그램으로 분류된다.

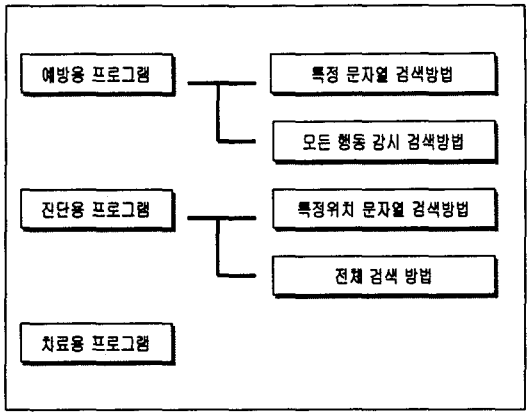

그림 1. 안티바이러스 프로그램 동작원리

예방용 프로그램은 컴퓨터 바이러스보다 먼저 메모리에 상주하여 모든 실행파일에 대해 바이러스 감염여부를 확인하게 되는데, 감염여부 검색은 방법에 따라 특정 문자열 검색방법과 모든 행동 감시 검색방법으로 분류된다.

진단용 프로그램은 바이러스 샘플에서 분석된 진단 문자열을 모든 파일에 비교 검색하여 문자열 존재 여부를 확인하게 되는데 그 방법으로는 특정 위치 문자열 검색과 전체 검색 방법이 있다.

치료용 프로그램은 원래의 복구 정보를 알아내어 원래 데이터를 기록함으로 감염 전의 상태로 복구시키는 동작이 이루어지는데 이때, 복구하지 못할 경우 삭제 여부를 확인하여 파일을 삭제한다.

3.4 연구 활동

안티바이러스 연구를 위한 활동으로 공개 사이트 검색 및 교내 바이러스 감염 컴퓨터를 통한 바이러스 샘플 수집, 바이러스 어셈블리 소스코드 분석, 국내외 안티바이러스 3종의 벤치마킹테스트, 공개 안티바이러스 소스 검색 및 분석 등이 이루어져 왔다. 이 활동 중 안티바이러스 3종의 벤치 마킹 과정에 대해서 좀 더 자세히 기술하겠다.

3종의 안티바이러스 엔진은 안철수 연구소의 V3, 하우리의 바이로봇, 시만텍의 노턴 안티바이러스이며, 엔진 비교에 앞서 우선 동일한 환경을 구성하였다. 같은 사양의 PC 3대를 준비해 각 PC에

서로 다른 안티바이러스 엔진을 설치하고, 3대의 PC를 하나의 네트워크로 구성했다.

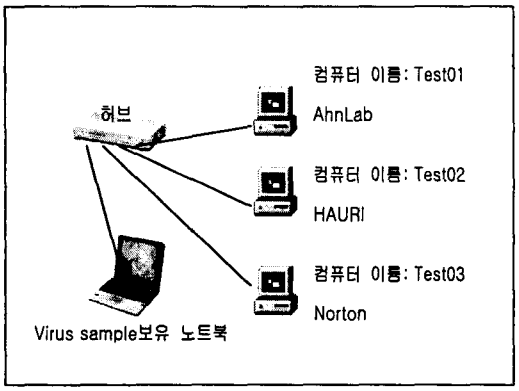

그림 2. 안티바이러스 성능 비교 환경도

그리고 바이러스 샘플을 담고 있는 노트북을 연결하여 각각의 PC로 똑같은 바이러스 샘플을 보내어 수동검사 진단 성능 및 치료성능, 압축 파일 진단성능, 시스템 감시기능, 업데이트 방법을 서로 비교하여 검사하였다.

3종의 안티바이러스 엔진 벤치마킹을 통해 각 안티바이러스 엔진의 진단성능 및 치료성능과 같은 기능적 특징을 알 수 있게 되었다. 검사 결과 압축파일 검사와 실시간 감시기능의 경우 거의 동일한 결과가 나오는 반면, 수동검사 진단 및 치료 성능에 있어서는 차이가 남을 알 수 있었다. 시만텍의 노턴 안티바이러스의 경우 나머지 두 엔진에 비해 진단률은 높으나 진단 바이러스의 절반도 치료하지 못하는 저조한 치료율을 보이는 반면, 국산 엔진인 안철수 연구소의 V3와 하우리의 바이로봇의 경우 진단률은 노턴 안티바이러스에 비해 현저히 낮으나, 진단 바이러스에 대한 치료율은 절반 이상으로 나타났다.

3.5 향후 연구 방향

웜(Worm)에 대한 더 자세한 지식을 얻기 위해, 웜 바이러스 소스를 분석하며, 계속 늘어나는 바이러스들에 대한 특징 및 동작원리에 대한 조사를 통해 최신 바이러스 동향을 분석하고, 문서화하여 DB로 구축할 것이다. 그리고 현재 진행중인 오픈 안티바이러스 소스 분석을 계속 해 나갈 것이며, 분석을 통해 나아가서는 그것을 응용한 바이러스 진단 모듈을 만드는 것이 최종 목표이다.

Ⅳ. 결론

CERTCC-KR에서 1월 25일 긴급경보를 내린 MS-SQL 서버 웜 슬래머(Slammer)의 공격[4]이 발생했을 당시 사전에 예측하지 못해 전세계 인터넷이 마비되었던 사건, 지난해 12월 공개한 지 하루만에 해킹을 당하면서 10억원의 투자비를 고스란이 날렸던[5] 성현아 누드사이트 해킹 사건, 국내 최대 결혼 정보회사인 듀오의 인터넷 사이트 해킹으로 인해 회원 30만명의 개인 정보가 유출된 사건[5] 등 끊이지 않고 많은 해킹 바이러스 관련 사고가 일어나고 있다. 그리고 사건들로 인한 피해의 규모도 실로 엄청나다.

이렇듯 인터넷 정보사회에서 자신의 정보를 해커로부터 지키고, 웜이나 악성 프로그램들로부터 자신의 PC를 지키는 일이 자신의 정보의 유실과 경제적 손실로부터 벗어날 수 있는 길이며, 해킹이나 악성코드에 의한 피해를 입었을 때에는 그것을 복구하고, 또 다시 피해를 입지 않도록 패치 설치나 엔진 업그레이드 등과 같은 취해야 할 방법에 대해 알고 있어야 한다. 그러나 현실은 그렇지 못하다는 것이 문제이다.

일반 사용자를 위한 정보보안 교육이 이루어지지 않고 있을 뿐만 아니라, 보안 회사의 제품을 설치하고, 관리를 받고 있는데도 해킹을 당하는 것이 현실이다.

따라서 정보보안 관련 연구활동 지원이나, kucis와 같이 대학생들로 이루어진 젊은 정보보안 인력을 키워나가는 것이 계속 되어야 한다.

참 고 문 헌

[1] 안철수, "바이러스 분석과 백신 제작", 정보시대, 1995
[2] 최주영, "인터넷 서버용 병렬처리 안티바이러스 엔진 설계", 서울여대 석사학위논문, 2002
[3] 안철수연구소, http://home.ahnlab.com
[4] CETCC-KR, http://certcc.or.kr
[5] 엠파스뉴스, http://news.empas.com