한국전산원장상

Network Guard System

1. S/W명 : Network Guard System

(클라이언트의 동작을 감시하여 유해한 인터넷 사이트에 접속하거나 불건전 프로그램을 수행하는 클라이언트에 대해 제재를 가하는 시스템)

2. 제작자 및 개발 과정 : 상명대학교 전자계산학과

본 시스템을 개발하는데 총 4인(교수 1인과 3인의 학부생)이 투입되어 방학 동안의 준비기간을 포함하여 5 개월(20 M/M)이 소요되었다. 본 시스템은 현재 상명 대학교 전자계산학과에서 진행 중인 '소프트웨어 공학' 과목의 term project의 산물이다. 개발 참여자와 그 역할은 표 1과 같다.

표 1. 개발자 및 역할

성 명	직 위	역 할	전화 번호
백 선 욱	교 수	총괄 지도 및 방향 설정	0417)550-5462
강 명 구	전산과 3학년	클라이언트 용 에이전트 개발	0417)550-5436
김 동 한	전산과 3학년	유해정보 데이터 베이스 구축	0417)550-5436
김 태 양	전산과 3학년	유해정보차단 서버/LSP 개발	0417)550-5436

주소 : 330-180) 충남 천안시 안서동 상명 대학교 전자계산학과

3. S/W 전체 요약 설명

(1) 개발 배경

최근에 인터넷의 효용성이 인식되기 시작하면서 가정이나 교육기관 및 회사 등에 인터넷이 급속도로 보급되고 있다. 그러나, 인터넷을 통해 음란, 폭력, 도박 등의 유해한 정보까지도 아무런 선별 없이 제공됨으로써 사회적으로 심각한 문제로 대두되고 있다.

즉, 가정에서 부모가 집을 비운 사이에 미성년 자녀들이 유해한 인터넷 사이트에 함부로 접근한다면 문제가 아닐 수 없다. 또한, 초등학교, 중, 고등학교 등 미성년자가 있는 환경이나 교회, 성당, 사찰 등의 종교 기관과 같은 환경에서 유해한 인터넷 사이트에 아무 제약 없이 접근할 수 있다고 한다면 심각한 문제가 아닐 수 없다. 한편 회사에서도 직원이 근무시간에 업무와 무관한 사이트에 접근한다면 업무 효율을 기대할 수 없다.

또한, 유해한 인터넷 사이트에 접근하지 않는다 하더라도 자신의 PC에서 교육시간이나 업무 시간에 교육/업무와 무관한 게임 등을 할 수도 있다.

본 소프트웨어는 클라이언트의 동작을 감시하여 유해한 인터넷 사이트에 접근하면 접근을 차단하고, 유해한 사이트에 접근하지는 않는다 하더라도 불량 게임 등, 관리자가 보기에 옳지 않은 행동을 하는 클라이언트는 강제로 시스템 종료시키는 등의 방식으로 제재를 가하는 시스템이다.

본고의 구성은 다음과 같다. 본 절의 아래 부분에서는 본 팀에서 개발한 시스템의 개요와 시스템 구성도 및 주요 기능에 대해서 기술하였다. 4절과 7절까지는 개발 일정과 개발 환경 및 수행 환경에 대해 기술하였으며, 8절과 9절에서는 본 시스템의 활용 방안 및 기대 효과에 대해 기술하였다.

(2) 개요

클라이언트의 불건전한 행동을 제재하기 위해 본 시스템에서는 유해한 사이트에 대한 데이터 베이스를 이용하는 방법과 클라이언트의 화면을 서버가 감시하는 방법의 두 가지가 서로 보완적으로 사용되고 있다.

유해한 사이트로의 접근을 차단하기 위해 클라이언트가 접근하고자 하는 인터넷 주소나 URL을 알아내어 그 주소가 유해한 사이트이면 접근을 거부하도록 하였다. 이때 특정 주소가 유해한 인터넷 사이트인지 아닌지를 판단하기 위해서 유해한 사이트의 목록을 저장한 데이터 베이스를 구축하였다.

클라이언트가 접근하려는 인터넷 사이트를 알아내기 위해 본 시스템은 Winsock2의 LSP(Layerd Service Provider)를 이용하였다. LSP는 TCP/IP 프로토콜에서 Winsock 계층과 아래의 TCP/IP 계층 사이에서 응용 프로그램이 하위의 TCP/IP로 내려보내는 메시지를 감시할 수 있는 기능이다(그림 2 참조). 따라서, 사용자가 web 브라우저 등을 이용하여 네트워크 인터페이스로 내려보낸 정보에 있는 URL이나 목적지 주소 등을 LSP 계층에서 잡아 유해 사이트 데이터 베이스를 참조하면 유해 사이트 여부를 알 수 있다. 유해하다고 판단되면 데이터를 하위의 네트워크 인터페이스로 전달하는 것을 거부하며, 그렇지 않은 경우만 밑으로 내려보낸다.

이렇게 LSP 수준에서 유해 정보 차단 기능을 구현하면 Web, Telnet, Ftp 등과 같은 응용 프로그램에 관계없이 차단 동작이 가능하다. 또한, 기존의 Winsock1.1에서 메시지 hooking 기능을 이용하는 것과는 달리 LSP를 한번만 설치하면 부팅 때마다 매번 실행시킬 필요가 없다.

전술한 방법대로 유해한 URL의 데이터 베이스(블랙 리스트)만을

가지고 유해정보를 차단하는 것은 완벽한 차단방법이 아니다. 왜냐하면 하루에도 새로운 유해사이트가 계속 생겨나기 때문이다. 그래서 본 시스템에서는 이런 점을 보완하기 위해서 클라이언트의 Window 화면을 Capture하여 서버에서 관리자가 볼 수 있게 하여 유해 정보로의 접근을 차단하고 강제종료 시킬 수 있게 하였다.

(3) 기능

- 인터넷 유해정보의 접근을 막아준다.
- LAN에 연결되어 있는 사용자 컴퓨터(클라이언트s)들의 작업화면을 감시한다.
- 관리자 컴퓨터(서버)에서 사용자 컴퓨터(클라이언트)로 경고 메시지 등을 보낼 수 있다.
- 계속 유해 정보로 접근한다면 관리자 컴퓨터에서 강제로 사용자 컴퓨터를 종료시킬 수 있다.

(4) 시스템 구성도

NGS의 시스템 구성도는 그림 1에 나타나 있는데, 클라이언트가 접속된 LAN에 이들의 동작을 감시하는 NGS 서버가 접속된다.

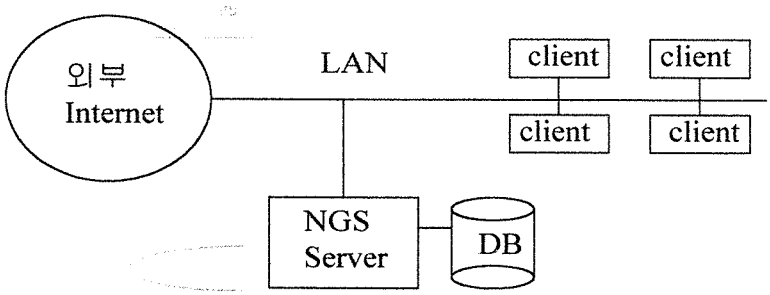

그림 1. NGS 시스템의 구성

NGS 서버는 유해한 사이트들에 대한 정보를 데이터베이스에 관리한다. 유해 정보 차단은 두 가지 방법으로 지원된다. 하나는 클라이언트가 접속하려는 사이트가 유해한 사이트인지에 대해 데이터베이스에 유해하다는 정보가 있으면 클라이언트 내의 LSP 프로그램이 접속을 차단하는 것이다.

두 번째 방법은 유해 정보 데이터베이스에 관련 정보가 없는 경우에도 적용할 수 있는 방법이다. 클라이언트에 미리 NGS 클라이언트용

에이전트(agent) 프로그램을 설치해 놓고 이 에이전트가 클라이언트의 수행 화면을 캡쳐하여 NGS 서버로 전송하면 서버는 이 화면을 보고 유해성 여부를 판단하여 클라이언트에게 경고 메시지나 강제 종료 메시지를 전송하는 방법이다. 이 방법은 클라이언트가 인터넷과 무관하게 stand-alone 불건전 게임을 하는 경우에도 사용될 수 있다.

이때, 클라이언트 내의 LSP 프로그램이나 에이전트 프로그램은 사용자가 함부로 지우지 못하도록 은닉하였다.

(5) 각 모듈의 기능

- URL에 의한 유해 사이트 접속 차단 시나리오(그림 2 참조)
  ① 클라이언트가 인터넷에 접속하여 URL을 입력한다.
  ② 클라이언트에 설치되어 있는 유해 정보 차단 LSP가 URL을 가로챈다.
  ③ 데이터 베이스에 있는 블랙 리스트(Black List)와 비교한다.
  ④ URL이 유해 사이트가 아니면 하위의 TCP/IP를 통해 접속을 허용하고 유해 사이트이면 클라이언트에게 경고 화면을 출력한 후 클라이언트의 응용 프로그램을 종료시킨다.

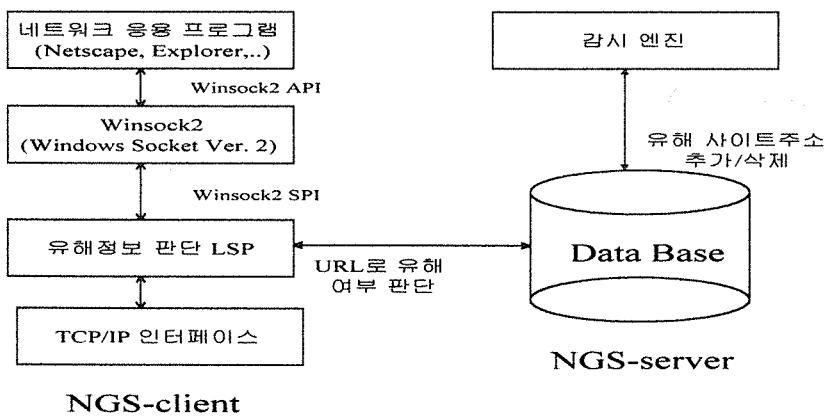

그림 2. URL에 의한 유해 정보 차단 구조

- 클라이언트의 작업 감시 기능
  ① 클라이언트 컴퓨터에 숨어 실행되고 있는 NGS-클라이언트 에이전트가 클라이언트 화면을 캡쳐하여 NGS-서버로 전송한다.
  ② NGS-서버는 데이터 베이스에 이 정보를 저장하며, 이 정보로

클라이언트 작업의 유해 여부를 판단할 수 있다.

- 클라이언트 제재.
  ① NGS-서버가 감시중인 클라이언트가 계속 유해 사이트에 접근하려고 시도하거나, 혹은 유해한 게임 등을 하는 것이 캡쳐 화면에 잡히면 먼저 경고 메시지를 전송한다.
  ② NGS-서버가 경고 메시지를 보냈는데도 클라이언트가 계속 유해 정보에 접근한다면 강제 종료 신호를 클라이언트로 보내어 NGS-클라이언트 프로그램에서 컴퓨터를 종료시킨다.

4. 개발단계별 기간 및 투입공수

본 시스템은 크게 서버, 클라이언트, 데이터 베이스로 구성되어 있는데, 4 명의 인원이 5개월간 개발하였다. 각 모듈별 세부 개발일정과 투입공수는 표 2와 같다.

5. 관계 프로그램 수

NGS 서버에서는 NGS 서버 엔진과 데이터베이스 프로그램의 두 부분, 클라이언트에서는 에이전트 프로그램과 LSP의 두 부분이 필요하여 총 4 개의 프로그램 군이 필요하다. 전체적으로 20 여개의 세부 프로그램으로 구성되어 있다.

6. 사용 또는 개발 언어, Tool

- 개발에 사용된 언어 :
  C, Visual C++ 6.0, Visual Basic 6.0, Delphi 4.0 Client/Server
- 개발에 사용된 Tool 및 기술:
  MS-SQL 서버 6.5, Winsock2 SDK, Sporder, RDO, LSP, Tray

7. 사용 시스템

개발에 사용된 시스템은 Pentium II 233 3 대이며 운영 체제는 Windows NT와 Windows 95환경에서 작업하였다. 실제로 설치하여 수행할 때는 NGS 서버는 NT를, 클라이언트는 Windows 98를 사용하였다.

표 2. 개발 단계별 기간 및 투입공수

항목 / 일정	6	7	8	9	10	투입공수 (M/M)
자료 조사						4
winsock구조 분석, 스키마 설계						2
화면캡쳐 구현, 사용자 DB 구축						2
서버GUI 코딩 및 Winsock2,LSP 분석						2
음란물차단기능 구현, Black List DB 구축						6
GUI 구현, 서버-클라이언트-DB 연동						1
프로그램 테스트, 통합						3
계	4인 * 5개월					20

8. 직접 효과

- 인터넷의 유해정보 접근을 차단해 줌으로써 청소년들의 건전한 인터넷 사용에 도움을 줄뿐 만 아니라 학교 및 사무실에서도 본래업무와 학업에 충실을 기할 수 있게 될 것이다.
- 회사 내에서 게임이라든지, 업무 외의 작업을 할 경우 관리자가 이를 차단해 줌으로써 업무의 능률을 극대화할 수 있다.

9. 간접 효과

- 청소년들로부터 인터넷 유해정보를 차단하여 올바른 인터넷 문화를 형성하게 된다.
- 회사에서 클라이언트의 행동 패턴을 수집 종합하여 분석함으로써 작업 생산성 향상 방안에 반영할 수 있다.
- winsock2의 LSP(Layerd Service Provider)를 이용함으로써 본 프로그램의 음란물 차단 해결뿐 아니라, 현재 인터넷의 Hacking으로 인해 중요시 되는 보안에 대한 새로운 해결책을 기대할 수 있게 되었다.

10. 결론 및 앞으로의 개발 방향

본고에서는 LAN에서 클라이언트를 감시하여 인터넷 상의 유해 사이트에 접근하거나, 혹은 인터넷에는 접근하지 않지만 클라이언트에서 유해한 작업을 하고 있을 때, 그 클라이언트에게 제재를 가할 수 있는 감시 시스템의 개발 내용을 정리하였다. 유해한 사이트의 목록은 데이터베이스에 유지되는데, 인터넷 상의 사이트에 클라이언트가 접근하여 하면 데이터 베이스를 참조하여 유해하다고 판단되면 접속을 차단한다.

데이터 베이스에 미처 등록되지 않은 유해 사이트도 있을 수 있으므로 이런 경우를 보완하기 위해 클라이언트에 에이전트 프로그램을 은닉하여 이 에이전트가 감시 서버에게 화면을 전송하도록 하였다. 서버는 이 화면을 보고 유해성 여부를 판단하여 클라이언트에게 경고 메시지를 보내거나 강제 종료시킨다.

유해 사이트에 대한 데이터 베이스가 충분히 구축되기만 한다면 현재 개발된 시스템은 실제로 유용하게 활용될 수 있을 것으로 예상된다. 따라서 앞으로는, 인터넷 상의 문서에 대해 검색하여 그 문서에 유해한 단어가 있으면 자동으로 데이터 베이스를 구축하는 기능을 더 추가할 예정이다. 또한, 다른 회사나 조직에서 보유하고 있는 유해정보 데이터 베이스를 공유하기 위한 방안도 개발할 예정이다.

한편 감시 기능을 강화하여 클라이언트의 제재 기능만이 아니라, 각 클라이언트의 내부 자원 사용 상황이나 트래픽 통계 등을 서버에서 수집하여 망 설계 및 관리에 활용할 수도 있도록 개발할 예정이다.