Journal of Korea Multimedia Society Vol. 13, No. 8, August 2010(pp. 1212-1220)

DB 보호를 위한 Protocol Redirection기반 트래픽 중앙통제시스템 개발

서양진[†], 이재필[††], 박천오[†††], 이덕규[††††], 장항배[†††††]

요 약

국내의 사용자 프로그램으로 Port Redirection 서버를 통해 주소 변환 정보를 받아 사용자의 트래픽을 변환시키는 기술은 미비하다. 일반적으로 네트워크 장비에서 구현되는 기술로써 네트워크 장비를 경유하여 입출력되는 트래픽에 대해 특수한 목적으로 활용하는 네트워크 기술의 일부이다. 이러한 특수 목적을 달성하기 위한 L4 Switch 장비와 네트워크 구조에 따라 여러 대의 추가적인 비용들이 발생한다. 이러한 문제점을 개선하기 위하여 단말기의 Network Layer에서 L4 스위치의 Redirection기능을 구현하여 네트워크 구조에 관계없이 원하는 Traffic을 한 곳으로 집중시켜 통제와 모니터링을 중앙 집중하여 관리할 필요성이 있다. 따라서, 본 논문에서는 Client 단에서의 Protocol Redirection을 통한 트래픽의 중앙통제시스템을 제안하고자 한다.

Development of Traffic Centralized Control System Based on Protocol Redirection for DB Protection

Yangjin Su[†], Jaepil Lee[††], Cheono Park[†††], Deokgyu Lee[††††], Hangbae Chang[†††††]

ABSTRACT

The technologies of domestic user programs are not enough to convert address convert information, which was collected via port redirection server, to user traffic. Generally traffic redirection technology is a special purpose technology for I/O traffic via network device. L4 switch needs various additional costs and devices to achieve this special purpose. To solve this problem, there appears need for a central management of control and monitoring by centralizing traffic at one position regardless of network structure and it is necessary to realize redirection function of switch at network layer. Therefore this study offer development of traffic central control system through protocol redirection of client-side.

Key words: DB Protection(DB 보안), Data Leakage(정보유출), Protocol Redirection(프로토콜 재 방향 설정), Traffic Control(트래픽 통제)

1. 서 론

컴퓨터 및 인터넷에 대한 의존도가 나날이 높아지고 있는 상황에서, 시스템의 취약성을 공격하는 해킹 방식은 대규모의 트래픽을 발생하여 네트워크 자체에 대해 위협적인 존재로 발전하고 있다[1]. 따라서

※ 교신저자(Corresponding Author) : 장항배, 주소 : 경기도 포천시 선단동 산11-1(487-711), 전화 : 031)539-1752, FAX : 031)539-1750, E-mail : hbchang@daejin.ac.kr
접수일 : 2010년 3월 17일, 수정일 : 2010년 5월 28일
완료일 : 2010년 6월 6일
[†] 정회원, 소프트캠프(주) 정보보안기술연구소 팀장
(E-mail : yjseo@softcamp.co.kr)
[††] 정회원, 소프트캠프(주) 부사장
(E-mail : jplee@softcamp.co.kr)
[†††] 정회원, (주)피앤피씨큐어 대표이사
(E-mail : copark@pnpsecure.com)
[††††] 종신회원, ETRI 지식정보보호연구부
(E-mail : deokgyulee@gmail.com)
[†††††] 종신회원, 대진대학교 경영학과 조교수

이러한 사이버 위협을 차단하고 예방하기 위한 다양한 네트워크 보안 제품들이 등장하고 있다.

개인정보 유출 사고의 증가와 이에 대응한 법률 등이 속속 시행되고 있고 고객정보 보안이 기업, 관공서에서 주요 키워드로 등장하고 있어 네트워크상의 모든 트래픽에서 중요한 정보를 가지고 있는 트래픽만을 선별적으로 관리하는 기술의 필요성이 더욱더 증가되고 있다[2,3].

국내의 사용자 프로그램으로 Port Redirection 서버를 통해 주소 변환 정보를 받아 사용자의 트래픽을 변환시키는 기술은 미비하다. 일반적으로 트래픽 redirection 기술은 router, L4 Switch와 같은 네트워크 장비에서 구현되는 기술로써 네트워크 장비를 경유하여 입출력되는 트래픽에 대해 특수한 목적(NAT, Routing)으로 활용하는 네트워크 기술의 일부이다[4].

단말기와 서버 사이의 통신에서 통제이나 모니터링, 기타의 목적으로 L4스위치를 이용하여 통신경로를 목적지 IP나 목적지 Port를 보고 양쪽 단말기상의 통신을 임의의 장비로 Redirection를 하여 소기의 목적을 달성하였다. 하지만 L4 Switch와 네트워크 구조에 따라 여러 대의 추가적인 장비들을 필요로 한다[5]. 이러한 문제점을 개선하기 위하여 단말기의 Network Layer에서 L4 스위치의 Redirection기능을 구현하여 네트워크 구조에 관계없이 원하는 고객정보 등의 트래픽을 한 곳으로 집중시켜 통제와 모니터링을 중앙 집중하여 관리한다. 이는 물리적인 구성에 관계없이 대용량의 트래픽 중에서도 중요한 정보가 삽입 되어 있는 트래픽만을 선별하여 관리할 수 있다[6,7]. 따라서, 본 논문에서는 Client 단에서의 Protocol Redirection을 통한 트래픽의 중앙통제시스템을 제안하고자 한다.

2. 선행연구

2.1 국내외 연구

국내에서는 사용자 프로그램으로 Port Redirection 서버를 통해 주소 변환 정보를 받아 사용자의 트래픽을 변환시키는 기술은 미비하다. 일반적으로 트래픽 redirection 기술은 router, L4 Switch와 같은 네트워크 장비에서 구현되는 기술로써 네트워크 장비를 경유하여 입출력되는 트래픽에 대해 특수한 목적(NAT, Routing)으로 활용하는 네트워크 기술의 일부이다[8].

국외에서는 Linux에서 유사한 기능으로 TCP 또는 UDP 서비스 포트를 다른 컴퓨터의 포트로 이양하여 자신의 서비스를 다른 컴퓨터에서 할 수 있도록 해주는 기능이 있다. 이는 주로 보안 강화에 용이하게 사용되며, 서버의 서비스 포트를 내부 네트워크를 사용하는 서버에 이양시켜 주어 크래커가 크래킹을 하지 못하여 서버의 데이터를 보호하는 방법으로 사용된다[9]. 관련 유틸리티로는 리눅스 커널 2.2에서 주로 사용하였던 ipmasqadm과 ipchains, iptables이 있다. 이것에 대해 용도로는 Routing, NAT등의 방화벽을 위한 도구로써 사용되며, 특정 프로토콜을 분석하기 위한 목적으로서 사용되는 것은 아니다[10].

3. 설계 및 구현

그림 1 port redirection을 통한 중앙 통제 시스템 개념처럼 이용자 환경의 변화 없이 중요 트래픽을 중앙 통제 시스템으로 트래픽을 redirection하여 단일 서버로 통합 관리를 할 수 있는 중앙 통제 시스템을 제안한다. 이는 특정 프로토콜 즉, DBMS, FTP, Telnet등의 프로토콜에 대해 중앙 서버로 redirection 하며 기존의 DB 게이트웨이에 의해 사용자의 명령을 모니터링 하고, 제어하는 시스템이다.

그림 2와 같이 사용자가 Telnet을 이용하여 192.168.200.200으로 접속을 시도하고자 하면, 정책을 통해 protocol redirection기능을 수행하는 사용자 프로그램(이하 NAT Client라 칭한다.)에 의해 목적지 주소를 중앙 통제 서버인 192.168.100.100으로 변경하여 처리한다. Telnet을 이용하여 접속하고자 하는 패킷은 중앙 통제 서버로 접속하게 되고, 중앙 통제 서버에서는 이에 대한 접속을 telnet 서버인 192.168.200.200으로 접속을 대신하여 준다. 이 때 보안 게이트웨이에 의해 사용자의 telnet 명령은 감시, 제어가

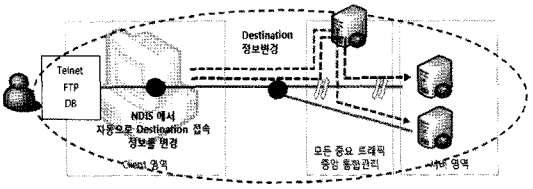


그림 1. port redirection을 통한 중앙통제 시스템 개념도

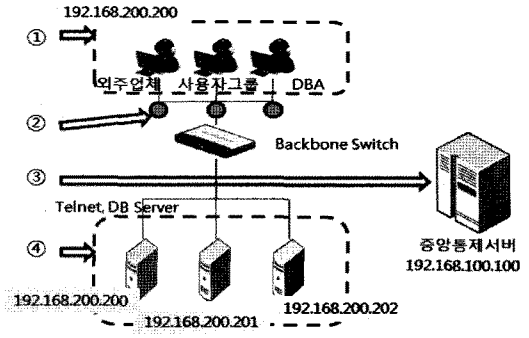


그림 2. 트래픽 중앙 통제 시스템으로의 protocol redirection 동작 방식

되며 사용자의 의심스러운 행동을 사전에 제어하며, 사후 추적 가능하도록 한다.

또한 이것에 대한 구체적인 패킷의 변화 과정은 그림 3과 같이 Network Layer 에서 동작하며 중요 패킷일 경우에만 Network Layer에서 목적지 IP (192.168.200.200)를 중앙통제서버로 Redirection 하기 위하여 목적지 IP를 192.168.100.100으로 변경한다.

본 논문에서 제안하는 시스템은 사용자의 트래픽 Redirection Agent는 중앙 통제 서버로 부터 주요 서버에 대한 정보를 내려 받으며, 주요 서버에 접속하려는 사용자의 프로토콜을 Redirection 기술을 이용하여 보안을 위한 감시를 할 수 있도록 하였다.

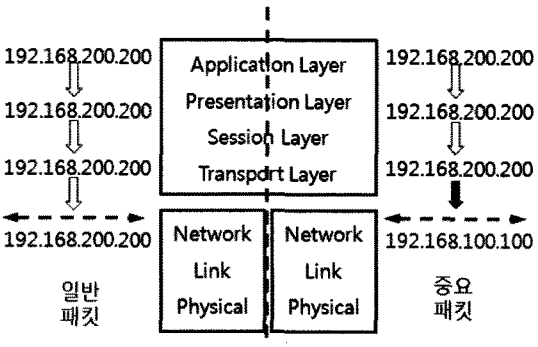


그림 3. OSI 7 Layer 상의 protocol redirection 과정

3.1 시스템 주요 모듈

본 논문에서 제안하는 시스템의 주요 모듈인 Protocol Redirection을 통한 중앙 통제 시스템 중 사용자 프로그램의 주요 구성 모듈은 그림 4와 같이 5가지 모듈로 구성된다.

정책 수신 모듈은 중앙 서버로부터 특정 프로토콜

정책 수신 모듈	사용자 관리 모듈
커널 제어 모듈	
NAT 정책 관리 모듈	
NAT 변환 모듈	

그림 4. 사용자 프로그램의 주요 모듈 구성

에 대해 NAT 동작할 리스트를 얻으며, 이에 대해 메모리에서 저장 및 관리하도록 한다. 사용자 관리 모듈은 사용자의 UI로써 수신된 정책의 동기화 및 프로그램 종료등의 역할을 담당한다. 커널 제어 모듈은 NAT 동작을 수행할 커널 모듈과의 통신을 담당한다. 이 때 중앙 통제 시스템으로부터 받은 정책을 커널모듈에 전달 및 게이트웨이의 MAC등을 전달한다. NAT 정책 관리 모듈은 커널 모듈의 일부로써 사용자 모듈에서 수신된 정책과 MAC등의 리스트를 관리한다. NAT 변환 모듈은 사용자 프로그램에서 NAT 기능을 하는 주요 모듈로써 패킷의 송수신시 NAT 정책 관리 모듈을 통해 변조할 패킷인지 비교 및 변조하는 모듈이다.

3.2 정책 수신 모듈

정책 수신 모듈은 정책수신, NAT 정보 관리, Gateway 변경 감지의 세부분의 구성으로 구성하였다.

정책 수신은 사용자 관리 모듈에서 설정된 정책 동기화 주기에 의해 주기적으로 소켓 통신을 이용하여 중앙 통제 시스템에 접근하여 정책 목록을 수신한다. 이 때 변경된 정책이 없으면(Serial Code로 체크) 수신하지 않는다. 주기적으로 정책을 수신하게 되면 다음의 NAT 정보 관리 모듈로 데이터를 저장하게 되며, 변경된 NAT 정책을 수신하기 전까지는 계속해서 메모리에 보관한다.

NAT 정보 관리는 정책 수신 모듈에 의해 수신된 NAT 정책을 관리한다. 보관 중인 NAT 정책 중 변경된 정책만 업데이트한다. 그림 5와 같이 변경된 NAT 정책을 검색 및 업데이트 시 복잡도는 O(n2)의 비교 검색이 된다. NAT할 정책 즉, 중앙 집중화 시킬 프로토콜 정보는 특정 프로토콜(DBMS, Telnet, FTP등)에 국한되어 있기 때문에 정책의 개수는 많지가 않다.

Gateway 변경 감지는 게이트웨이의 MAC은 NAT 주소 변환 시 매우 중요하기 때문에 중앙 통제 시스템이 라우터와 같은 게이트웨이의 외부에 위치하여

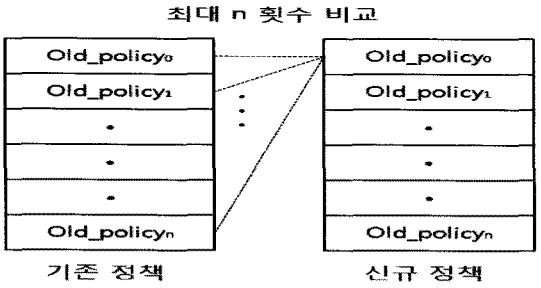


그림 5. 정책 수신 및 업데이트 과정

있을 경우 잘못된 MAC Address의 주소는 도달할 수 없는 경우가 발생할 수 있고 게이트웨이의 주소 변경 시 이를 재 설정하도록 하였다. Windows API 함수의 DWORD NotifyRouteChange(PHANDLE Handle, LPOVERLAPPED overlapped); 는 이를 감지하여 주는 역할을 한다. 이 때 Router의 주소 즉, 게이트웨이의 주소 변경 감지 이벤트를 받게 되면 이를 커널 제어 모듈에 신속하게 설정할 수 있도록 커널 제어 모듈을 호출한다.

3.3 사용자 관리 모듈

사용자 관리 모듈은 UI와 환경 정보를 읽어오는 부분으로 구성하였다. UI 부분은 정책 수신 모듈에 의해 수신된 정책 목록과 사용자 프로그램 종료 및 정책 동기화 기능을 수행한다.

환경 정보에서는 사용자 프로그램의 환경 설정 정보 파일을 읽어 정책 동기화 주기, 중앙 통제 시스템의 주소 및 각종 환경 정보를 읽어 커널 제어 모듈과 정책 수신 모듈과 통신을 한다. 아래의 표 1과 같이 환경 정보 목록이 있으며, 본 연구 수행 및 적용 시 많은 요구 사항과 함께 추가된 정보이다.

3.4 커널 제어 모듈

커널 제어 모듈은 수신된 정책을 받아 커널 통신 모듈에 전달하는 정책 통신 모듈과 커널에 정책을 전달해 주는 커널 통신 모듈로 구성하였다.

정책 통신 모듈은 정책 수신 모듈에 의해 관리되어 있는 게이트웨이 MAC과 정책 목록을 받아 커널 통신 모듈에 전달한다. 이 때 전달되는 정책 목록 갱신 시 변경된 정책만 반영이 되도록 커널 모듈이 가지고 있는 정책과 비교한다. 또한, 커널 모듈이 작동 중지, 프로토콜 변환 작업 중지등의 요청에 대해 처리하도록 한다. 커널 통신 모듈과의 통신 시 프로토콜을 정의함으로써 표 2와 같이 약속된 규약에 의해 운영되도록 한다.

표 1. 한경 설정 정보

항 목	설 명
Port	중앙 통제 시스템과의 통신을 위한 접속 포트
Interval	정책 동기화 주기
RetryInterval	정책 동기화 실패 시 재접속 주기
RetryCount	정책 동기화 실패 시 재접속 시도 횟수
Resolve	IP 또는 DNS에 의한 중앙 통제 시스템의 위치 설정
FailOff	장애 발생 시 Fail Over 또는 Fail Open할 지의 여부
LoadBalance	Load Balance를 할지 여부(중앙 통제 시스템의 여러 개일 경우 임의 선택 가능하도록 한다.)
ShowDBSAFER	DB 보안 시스템의 주소 및 포트 정보를 보일지의 여부
DNSIP	Resolve option이 dns 로 설정 시 중앙통제시스템의 URL
IP1	중앙 통제 시스템의 주소로 최대 4개까지 입력 가능하다.

그림 6과 같이 통신 프로토콜 규약 설정 시 32bit의 값에 대해 매크로를 이용하여 설정된다. CTL_CODE의 매크로는 winioctl.h 파일에 아래와 표 3 CTL_CODE 처럼 정의하였다.

커널 통신 모듈은 사용자의 정책 수신, 드라이버의 작동, 중지 등의 명령을 처리하기 위한 중계 역할을 한다. 이러한 처리를 위한 루틴들을 디스패치 루틴이라 하며 각 Windows API 함수와 입출력 요구 사항에 대한 코드 및 처리 사항들에 대한 기술은 아래의 표 4와 같다.

3.5 NAT 정책 관리 모듈

NAT 정책 관리 모듈 커널 제어 모듈의 커널 통신

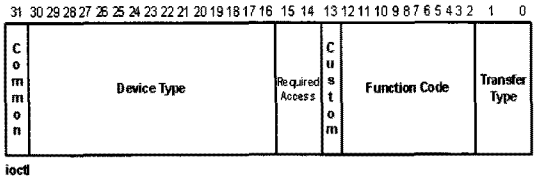


그림 6. IO Control code layout

표 2. 커널 모듈과의 통신 규약의 일부

```
#define IOCTL_SET_STATUS_NAT CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 2, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_GET_STATUS_NAT CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 3, METHOD_BUFFERED, FILE_READ_ACCESS)
#define IOCTL_SET_IP_NAT CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 4, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_CLEAR_IP_NAT CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 5, METHOD_BUFFERED, FILE_READ_ACCESS)
#define IOCTL_ADD_MAC_INFO CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 6, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_CLEAR_MAC_INFO CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 7, METHOD_BUFFERED, FILE_READ_ACCESS)
#define IOCTL_MODI_MAC_INFO CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 8, METHOD_BUFFERED, FILE_ANY_ACCESS)
// NAT Driver가 가지고 있는 MAC 정보의 총 갯수를 얻어온다.
#define IOCTL_GET_MAC_SIZE_INFO CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 9, METHOD_BUFFERED, FILE_ANY_ACCESS)
// NAT Driver가 가지고 있는 MAC 정보를 얻어온다.(IN: MAC 정보의 위치(0 based index), OUT: MAC 정보 (_stMACData_)
#define IOCTL_GET_MAC_INFO CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 9, METHOD_BUFFERED, FILE_ANY_ACCESS)
#define IOCTL_SET_DEBUG CTL_CODE(FILE_DEVICE_UNKNOWN, IOCTL_Start + 100, METHOD_BUFFERED, FILE_ANY_ACCESS)
```

표 3. CTL_CODE의 정의

```
#define CTL_CODE( DeviceType, Function, Method, Access ) (                \
((DeviceType) << 16) | ((Access) << 14) | ((Function) << 2) | (Method) \)
```

모듈로부터 받은 정책을 저장하는 부분과 해당 정책을 NAT을 위한 비교하는 모듈로 구성되어 있다. 정책 저장소에서 정책 항목은 리스트의 형태로 관리하며, 관리되는 리스트의 구성 항목은 표 5와 같다.

패킷 송수신 시 처리과정은 패킷의 송수신이 감지되면 패킷의 TCP/IP 헤더의 IP/Port와 정책을 비교 후 프로토콜의 MAC, IP, Port 변경을 한다. 그리고, 변경이 완료되면 체섬을 계산 후 변경 및 송수신하도록 한다. 불일치하면 Protocol Redirection할 대상이 아니므로 그대로 패킷의 방향대로 진행하도록 한다.

3.6 NAT 변환 모듈

NAT 변환 모듈은 NAT 변환 모듈은 패킷 송신 시 처리하는 모듈과 패킷 수신 시 처리하는 모듈로 구성되어 있다. 패킷 송신 모듈은 사용자가 DBMS 또는 텔넷을 이용하여 접속하고자 할 때, 즉 중요 프로토콜을 이용하려 할 때 데이터를 서버에 보내게 된다. 이 때 패킷을 서버로 보내게 되는데, 패킷 송신 모듈에서는 다음과 같은 원리에 의해 패킷을 변조하며 송신하게 된다.

그림 7과 같이 순차적으로 패킷이 Ethernet Frame ->IP Packet->TCP Packet을 붙여가며 진행하며, 그림 8과 같이 Packet과 Buffer를 할당한다.

또한 그림 9와 같이 NdisAllocateBuffer는 이미 할당된 비 페이지화된 메모리 블록내에 특정 가상 범위(range, 영역)와 맵핑하는 버퍼 디스크립터를 만든

표 4. 디스패치 루틴 및 역할

Win32 함수	IRP 주요 코드	처리 사항
CreateFile	IRP_MJ_CREATE	NAT Driver open할 경우 처리
CloseHandle	IRP_MJ_CLOSE	NAT Driver close할 경우 처리
ReadFile	IRP_MJ_READ	NAT driver를 읽을 경우(파일 처럼 handling)
WriteFile	IRP_MJ_WRITE	NAT driver에 무언가를 write할 경우
DeviceIoControl	IRP_MJ_DEVICE_CONTROL	기타 부가적인 정보를 read/write할 경우 해당 부분에 대한 처리에서 정책, 수신 등의 각종 정보를 이용한다.

표 5. Protocol redirection을 위한 정책 항목

항 목	내 용
목적지 IP	변경하고자 하는 대상 서버의 IP 즉, 해당 IP에 대해 중앙 집중 서버 IP로 변경한다.
목적지 Port	변경하고자 하는 대상 서버의 Port
서버 IP	중앙 집중 서버의 IP
서버 Port	중앙 집중 서버의 Port
NAT 여부	프로토콜 변환 할지의 여부
MAC 주소	Gateway MAC 주소

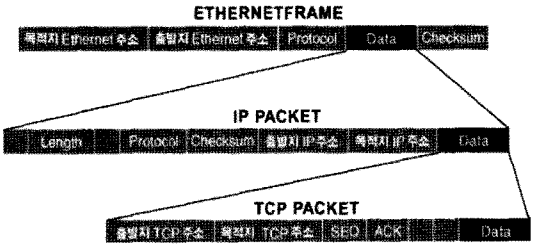


그림 7. 패킷의 흐름

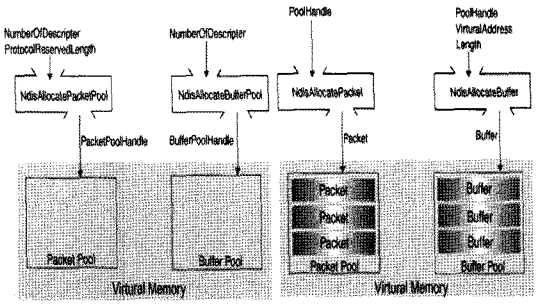


그림 8. Windows 커널에서의 패킷의 할당 과정

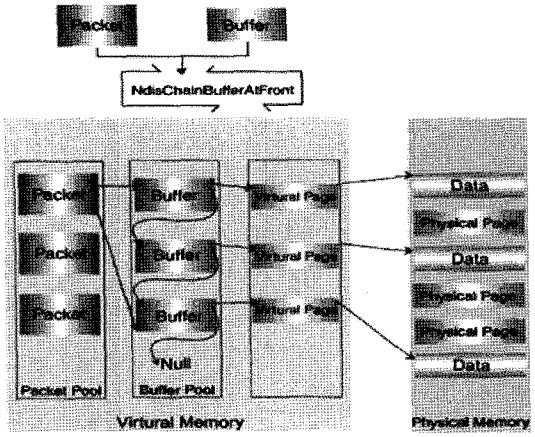


그림 9. 버퍼 디스크립터 생성 및 송신

다. NDIS_BUFFER는 일반적으로 3개 이다. 데이터를 3부분(Ethernet Header, TCP/IP Header, Data)으로 나눠서 보내기 때문에 Buffer를 3개 할당해서 각각의 데이터들의 선두 번지 값을 저장해 두는 것이며, 마지막으로 이렇게 저장된 데이터들이 하나로 묶여 NdisSend나 PacketSendCommand를 통해서 PROTOCOL에서 MINIPORT나 MINIPORT에서 다른 서버나 호스트로 전달되는 것으로 패킷 송신을 끝내게 된다. 패킷 수신 모듈은 변조된 패킷을 송신하고 나서 서버로 부터의 응답을 처리하도록 합니다. 이 때 사용자는 실제 서버와 통신하는 것처럼 보이게 하기 위해서 수신 과정에서 패킷을 DBMS 서버나 텔넷 서버의 주소, 포트 정보로 변조한다.

그림 10에서와 같이 수신에서도 송신과 구조적으로는 송신과 별반 차이가 없이 송신에서의 반대 순서로 수신과정이 이루어진다. 하지만 송신과 가장 다르다 할 수 있는 것은, 앞 송신에서는 하나의 패킷이 3개의 버퍼로 나누어져 메모리 공간상에 기억되었다 전송되었지만 수신에서는 하나의 버퍼에 하나의 패킷이 연결되는 것이 가장 큰 차이이다. 처음 NIC이 데이터를 수신하면 ReciveInterrupt를 발생시키고 MINIPORT ISR에 전달하고,받은 데이터를 물리 메모리에 저장하여 그에 대한 가상페이지에 그 기록을 저장한다. 이 ReciveInterrupt는 MiniportHandle-Interrupt Call을 호출해 다시 MiniportHandle-Interrupt에 전달이 되며, 이렇게 전달되어진 MiniportHandleInterrupt에서 MIndicateRecive Packet을 통해 패킷을 얻어오고 그 패킷은 Protocol-RecivePacket에 또다시 전달되어 진다. 여기에서는 NdisQueryPacket와 NdisQueryBuffer를 통해 가상주소를 얻고 그에 저장되어진 물리 주소를 찾아가

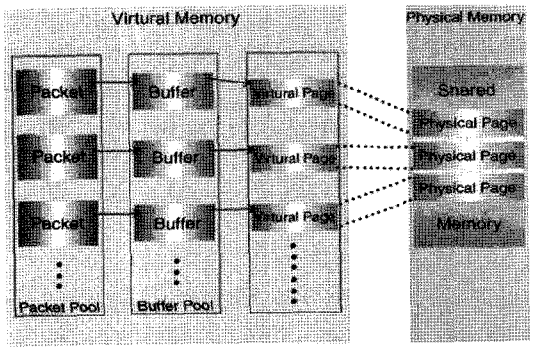


그림 10. 패킷 수신 과정

실제 수신한 데이터를 얻어온다. 그 데이터는 Protocol Stack에서 텔넷 또는 DBMS 응답 값의 데이터로 바뀌어 우리가 보는 화면에 나타나게 된다.

4. 실험결과

그림 11은 텔넷을 이용하여 192.168.2.128에 접속을 시도하였을 경우 Protocol Redirection의 기능을 수행하는 사용자 프로그램에 의해 수행되는 패킷의 전달 과정을 설명하고 있다. 사용자의 IP는 192.168.2.52이며, 텔넷 서버는 192.168.2.128의 주소와 23번의 포트를 가진다. 이 때 사용자는 텔넷 명령을 이용하여 접속 시도하게 되면 Windows 커널의 Protocol Redirection 기능을 통해 중앙통제시스템인 192.168.2.132로 forwarding을 하게 되며 중앙통제시스템에 의해 텔넷 서버로 연결, 수행하게 된다. 이 때 사용자의 PC에서 패킷 덤프와 사용자와 중앙통제시스템의 패킷을 덤프하여 비교하였다.

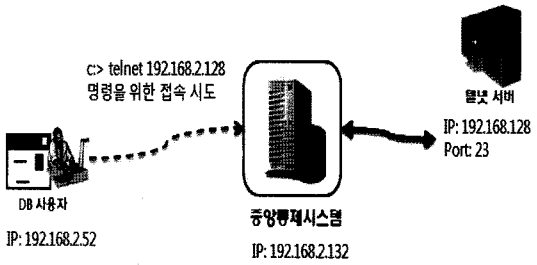


그림 11. 텔넷을 이용한 접속

그림 12는 사용자가 C:> telnet 192.168.2.128의 명령을 이용할 경우 사용자의 PC에서는 패킷이 변조되기 전의 패킷으로 보이게 된다. 즉 출발지 IP는 192.168.2.52가 되며 목적지는 192.168.2.128이 된다.

그림 13은 사용자와 중앙 통제 시스템간에 변조된 패킷이다. 즉, 출발지 IP는 192.168.2.52가 되며, 목적지의 IP는 192.168.2.132가 된다. 그와 같은 결과를 통해 Protocol Redirection 기능을 통해 중요 프로토콜에 대해 중앙 집중화를 시킴으로써 감시할 수 있는 것을 확인하였다.

그림 14는 본 연구에서 제시한 Client 단에서의 Protocol Redirection을 통한 트래픽의 중앙 통제 시스템의 실행 화면 중 Protocol Redirection을 위한 정책 목록이다.

5. 결 론

L4스위치를 이용하여 통신경로를 목적지 IP나 목적지 Port를 보고 양쪽 단말기상의 통신을 임의의

1	19:34:48.532868	192.168.2.52	192.168.2.128	TCP	51323 > telnet [SYN] Seq=0 Len=0 MSS=14
2	19:34:48.533103	192.168.2.128	192.168.2.52	TCP	telnet > 51323 [SYN, ACK] Seq=0 Ack=1 W
3	19:34:48.533218	192.168.2.52	192.168.2.128	TCP	51323 > telnet [ACK] Seq=1 Ack=1 Win=65
4	19:34:48.548439	192.168.2.128	192.168.2.52	TELNET	Telnet Data ...
5	19:34:48.548599	192.168.2.52	192.168.2.128	TELNET	Telnet Data ...
6	19:34:48.548866	192.168.2.128	192.168.2.52	TCP	telnet > 51323 [ACK] Seq=13 Ack=7 Win=5
7	19:34:48.548900	192.168.2.52	192.168.2.128	TELNET	Telnet Data ...
8	19:34:48.548919	192.168.2.128	192.168.2.52	TELNET	Telnet Data ...
9	19:34:48.588968	192.168.2.128	192.168.2.52	TCP	telnet > 51323 [ACK] Seq=16 Ack=16 Win=
10	19:34:48.589004	192.168.2.52	192.168.2.128	TELNET	Telnet Data ...
11	19:34:48.589302	192.168.2.128	192.168.2.52	TELNET	Telnet Data ...
12	19:34:48.589400	192.168.2.52	192.168.2.128	TELNET	Telnet Data ...
13	19:34:48.629949	192.168.2.128	192.168.2.52	TCP	telnet > 51323 [ACK] Seq=28 Ack=31 Win=

그림 12. 사용자 PC에서의 패킷 덤프

1	20:41:43.523867	192.168.2.52	192.168.2.132	TCP	52446 > 4011 [SYN] Seq=0 Len=0 MSS=1460
2	20:41:43.523919	192.168.2.132	192.168.2.52	TCP	4011 > 52446 [SYN, ACK] Seq=0 Ack=1 Wi
3	20:41:43.523993	192.168.2.52	192.168.2.132	TCP	52446 > 4011 [ACK] Seq=1 Ack=1 Win=6553
4	20:41:43.533122	192.168.2.132	192.168.2.52	TCP	[TCP segment of a reassembled PDU]
5	20:41:43.533249	192.168.2.52	192.168.2.132	TCP	[TCP segment of a reassembled PDU]
6	20:41:43.533522	192.168.2.132	192.168.2.52	TCP	4011 > 52446 [ACK] Seq=13 Ack=7 Win=584
7	20:41:43.533548	192.168.2.52	192.168.2.132	TCP	[TCP segment of a reassembled PDU]
8	20:41:43.533722	192.168.2.132	192.168.2.52	TCP	[TCP segment of a reassembled PDU]
9	20:41:43.534035	192.168.2.132	192.168.2.52	TCP	[TCP segment of a reassembled PDU]
10	20:41:43.534065	192.168.2.52	192.168.2.132	TCP	[TCP segment of a reassembled PDU]
11	20:41:43.574699	192.168.2.132	192.168.2.52	TCP	4011 > 52446 [ACK] Seq=28 Ack=25 Win=58

그림 13. Protocol Redirection 변환 후의 패킷 덤프

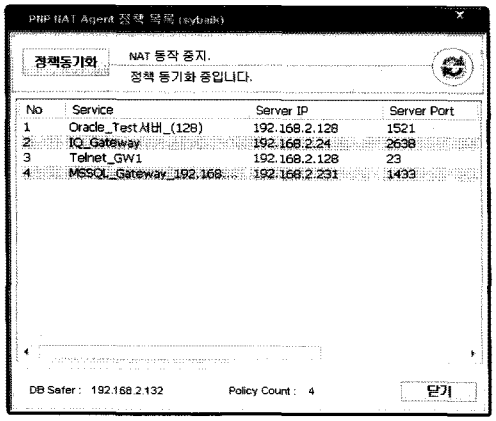


그림 14. 실행 프로그램 화면

장비로 Redirection한 방법의 경우 네트워크 구조에 따라 여러 대의 추가적인 장비들을 필요로 한다. 이러한 문제점을 개선하기 위하여 본 연구에서는 단말기의 Network Layer에서 L4 스위치의 Redirection 기능을 구현하여 네트워크 구조에 관계없이 원하는 트래픽을 한 곳으로 집중시켜 통제와 모니터링을 중앙 집중하여 관리하고 물리적인 구성에 관계없이 대용량의 트래픽 중에서도 우리가 중요하다고 생각하는 정보가 들어 있는 트래픽만을 관리할 수 있다는 TCP/IP 소켓레이어 기반 기술에 의거하여 동작되는 중요 프로토콜의 중앙 집중화를 시킴으로서 감시 및 제어 기능을 구현한 시스템을 개발하였다.

물리적인 네트워크 구성에 관계없이, 중요한 프로토콜에 대한 모니터링과 통제를 정확한 보안 정책을 구현 할 수 있어 현재의 보안 제품에서 할 수 없었던 자유로운 보안 통제가 가능 하므로, IDS, Firewall, Applicaion firewall, 및 IPS가 제공하지 못하는 보안 요소들에 대하여 완벽한 대안을 제시 할 수 있었다. 중요 프로토콜(TNS, Telnet,FTP,SSH) 사용이 많은 금융권/고객 서비스 사업분야 등의 보안 문제로 말생하는 개인정보/금융 거래내역 등의 유출에 따른 2차적 금전 손실을 사전에 방지 할 수 있으며, 국내외에서 사용하는 주요 프로토콜에 대한 보안을 견고하게 할 수 있어 새로운 틈새시증을 개척하며 IDS, Firewall 및 IPS 등이 제공하지 못하여 발생한 서비스 개발의 한계를 본사의 제품이 극복하게 하여 사업 전반에 걸쳐 다양한 성장이 이루어 질 것이라 기대한다.

참 고 문 헌

[1] 오승희, 남택용, 손승원, "네트워크 보안 동향," [IITA] 정보통신연구진흥원 학술정보.

[2] 오행석, 김정녀, 손승원, "차세대 네트워크 보안 표준화," 대한전자공학회, 전자공학회논문지, 제43권, TC편 제7호, pp. 122-13, 2006.

[3] 서정택, 윤주범, 임을규, 이철원, "네트워크 보안 시뮬레이터에 관한 연구," 한국정보과학회, 한국정보과학회 2002년도 가을 학술발표논문집, 제29권, 제2호(I), pp. 475-477. 2002.

[4] Bishop M. and Bailey D., "A Critical Analysis of Vulnerability Taxonomies," Technical Report CSE-96-11, Dept. of Computer Science, University of California at Davis, 1996.

[5] Brian Marick, "A Survey of Software Fault Surveys," Technical Report UIUCDCS-R-90-1651, University of Illinois at Urbana-Champaign, 1990.

[6] Eugene H. Spafford, "Common System Vulnerabilities," Proceedings of the Workshop on Future Directions in Computer Misuse and Anomaly Detection, 1992.

[7] Howard JD. "An Analysis of Security Incidents on the Internet," Ph. D Thesis, Carnegie Mellon University, 1997.

[8] Lee,Y. H. and Hwang, D. J., "Design and Implementation of Agent Based Dynamic Digital Rights Management," *Journal of Information Processing Association*, D. Vol. 8D, No.5, pp. 613-622, October 2001

[9] Lai, D. and Zhongwei Zhang, "Improving Efficiency and Scalability of Service Network Graph by Re-routing Service Routes," *Intelligent Information and Database Systems*, pp. 414-419, 2009.

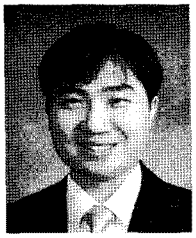
[10] Sairam A.S. and Barua G., "Distributed route control schemes to load balance incoming traffic in multihomed stub networks," Communications(NCC), pp. 1-5, 2010

서 양 진

1994년 중앙대학교 컴퓨터공학과 (학사)
1998년 중앙대학교 컴퓨터공학과 (석사)
2006년 중앙대학교 컴퓨터공학과 (박사 수료)
2002년~2003년 아시안사인(주) 전자거래연구원 팀장
2004년~현재 소프트캠프(주) 정보보안기술연구소 팀장
관심분야 : 정보보안, 시맨틱 기술, 정보검색, 인공지능

이 재 필

1987년 3월~1993년 2월 중앙대학교 전자계산학과(학사)
1993년 3월~1995년 2월 중앙대학교 컴퓨터공학과(공학석사)
1995년 3월~1999년 8월 중앙대학교 컴퓨터공학과(공학박사)
1994년 6월~1998년 12월 미래산업㈜ 선임연구원
1999년 7월~현재 소프트캠프㈜ 부사장
관심분야 : 정보보안(e-DRM,DB보안),인공지능(학습 및 추론)



박 천 오

2003년~현재 (주)피앤피시큐어 대표이사
관심분야 : 내부정보유출방지, 데이터베이스 보안

이 덕 규

2001년 순천향대학교 공학사
2003년 순천향대학교 공학석사
2006년 순천향대학교 공학박사
2006년~현재 한국전자통신연구원 지식정보보호연구부
관심분야 : 홈 네트워크, 키 관리, 항공자료 보안

장 항 배

2006년 2월 연세대학교 정보시스템 박사
2007년 3월~현재 대진대학교 경영학과 조교수
관심분야 : 산업보안, u 비즈니스 전략, 정보화(정보보호) 수준 및 성과평가