제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

내부 네트워크 보호를 위한 차단 지능형 TAP 의 설계

강유성*, 김종수*, 정기현*, 최경희**

*아주대학교 전자공학부, **아주대학교 정보통신 대학원
e-mail : kys11@madang.ajou.ac.kr

Designing A Smart TAP for Inter-Network Protection

Yousung Kang*, Jongsu Kim*, Kihyun Chung*, Kyunghee Choi**

*Dept. of EE, Ajou University
** Graduate school of I&E, Ajou University

요 약

인터넷과 네트워크 기술의 발달은 실생활에 많은 편리함을 주고 있지만 그에 따른 여러 가지 부작용들도 많이 나타나고 있다. 그 중 가장 심각한 문제는 보안 사고에 의한 피해인데, 최근에는 특정 장치를 해킹하여 자료를 망가뜨리는 것보다 불특정 다수에 의한 과다한 트래픽 생성 공격이 더 많아 지고 있다. 특히 DoS/DDoS(Distributed Denial of Service)와 같은 공격은 공격자가 네트워크 전문 지식을 가지고 있지 않아도 공격을 할 수 있고 원천적인 방어 방법이 없다는 점에서 심각성이 증대되고 있다. 본 논문에서는 네트워크 모니터링에 사용되는 TAP(Test Access Port)의 기반 기술을 이용하여 평시에는 TAP 의 본 기능을 수행하다 DoS/DDoS 공격과 같이 과다한 네트워크 트래픽 발생으로 장비가 멈추거나 망가지는 상황 등의 장애 발생시 내부 네트워크를 외부와 물리적으로 분리할 수 있는 지능형 TAP (S-TAP)에 대한 설계에 대해 설명하였다. 또한 S-TAP 을 이용하여 기존 네트워크에 적용될 수 있는 환경을 제시하여 S-TAP 의 유용성도 언급 하였다.

1. 서론

지금까지 네트워크 통신 기술과 인터넷은 서로의 인접한 관계에 의해서 동시에 질적, 양적으로 많은 발전을 이루어왔다. 세계 각 국가들이 정보화 고속도로를 구축 했거나 하고 있어 앞으로는 이러한 기술들이 더 빠른 속도로 발전하게 될 것이다.

하지만 이러한 급격한 양적 성장으로 인한 많은 문제점들이 사회적 문제로 가시화 되는 등 부작용이 증가하고 있다. 특히 해킹으로 인한 내부 정보들에 대한 외부 유출, 바이러스나 서비스 거부 공격 등에 의한 시스템의 서비스 중단 같은 경제적 피해들이 큰 폭으로 증가하면서 많은 관심을 받고 있다.

근래에는 해킹의 일종인 서비스 거부 공격(DoS: Distributed Denial of Service)에 대한 피해들이 크게 증가하고 있는데, 자료 절취와는 다른 성격으로 막대한 트래픽을 대상에 전달함으로써 정상적인 인터넷 서비스를 방해하는 방식이다. 2000 년 초에 amazon, eBay, Yahoo 등의 유명한 사이트들이 DDoS 공격을 받아 몇 일간 사이트 운영과 기업 이미지에 심각한 피해를 받는 사건 등이 그 예이다.[1] 서비스 거부 공격은 해킹에 비해 상대적으로 네트워크와 시스템에 대한 전문적인 지식을 가지고 있지 않은 공격자들도 비교적 쉽게 사용할 수 있는데 이는 프로그램 형태로 인터넷을 통해 쉽게 구할 수 있기 때문이다. 또한 웜(Worm)과 같은 프로그램들도 자기 복제를 하면서 네트워크에 큰 트래픽으로 작용하여 망을 거의 불능 상태로 만들기도 한다.[6] 지난 2003 년 1 월에 발생한 MS-SQL 취약점을 이용한 웜의 경우 전세계 주요 인터넷 선진국들에게 역대 가장 큰 통신 두절 사태를 맞게 하는 등

막대한 피해와 혼란을 주었었다.[7]

물론 이처럼 과다한 트랙픽을 발생 시키는 공격에 대한 방어 연구가 없었던 것은 아니지만 DDoS 공격에 대한 방어가 근본적으로 어려워 명확한 해결방법을 찾기가 어렵다. 그러므로 평상시에는 내부망을 외부망과 연결해 주고, DDoS 공격을 받을 때에는 각종 인터네트워킹 장비를 보호하고 내부 망만이라도 사용 할 수 있도록 하기 위해 외부 망과의 물리적 연결을 자동으로 단절 시키는 방법도 적절한 보안 대책이 될 것이다.

본 논문에서는 네트웍 모니터링 보조 장비인 TAP(Test Access Port)의 기반 기술을 이용하여 평상시에는 네트웍 트래픽 분석 장비와 연동하여 사용하고 그 장비들의 분석 결과에 따라 네트워크를 물리적으로 연결 시키거나 끊을 수 있는 S-TAP(Smart-TAP)장치의 설계에 대해 서술하였는데 서론에 이어 2 장에서는 망에 흐르는 트래픽을 모니터링하는 방법들에 대해 기술하였고, 3 장에서는 S-TAP 의 설계와 적용되는 네트워크 환경에 대해 기술 하였다. 4 장에서는 결론 및 향후 과제에 대해 논의하였다.

2. 관련 연구

최근에는 네트워크 보안 강화를 위해 방화벽에 이어 침입 탐지 시스템(IDS: Intrusion Detection System)도 많이 도입하고 있는 추세이다. 방화벽은 양 쪽 망의 교차 지점에 위치하고 있으며 오고 가는 모든 트래픽을 감당해야 하므로 성능의 제약으로 인해서 모든 트래픽의 분석을 할 수는 없다. 그래서 보안 솔루션에서는 방화벽의 취약점을 보안하기 위해 IDS 장비를 도입하여 사용하는 것이다.[4]

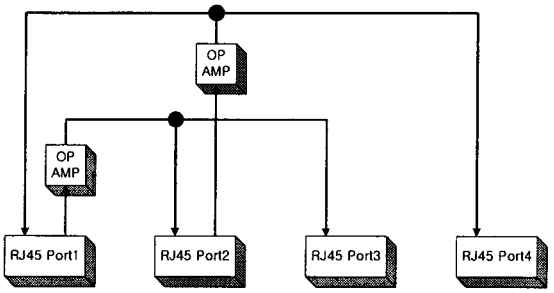
침입 탐지 시스템은 외부망과 내부망 사이를 흐르는 패킷들을 모두 감시하여 해킹이나 플러딩(Flooding) 공격과 같은 부적절한 행동을 분석하고 관리자에게 통보하는 역할을 하는데[2], 망에 영향을 미치지 않고 트래픽을 감시하기 위해 모니터링(Monitoring)을 수행해야 한다.

현재까지 논의된 주요 네트워크 모니터링 방법 및 기술에는 네트워크 종단점(Endpoint)인 PC 나 서버에서 패킷을 수집하는 방법, 더미 허브나 스위치의 포트를 감시하는 방법(Port mirroring), 수동적 TAP 장비를 이용하는 방법들이 있다.

네트워크 종단점에서 트래픽을 모니터링하는 방법은 패킷을 수집하고 분석하는 소프트웨어 모니터링 솔루션을 단말에 설치하여 구현할 수 있다. 이 방법은 가장 구현이 간단하며 추가적인 장치가 필요 없는 장점이 있다. 그러나 대부분의 네트워크에서 단말은 스위치와 연결되어 사용되므로 자신에게 혹은 자신으로부터 송수신되는 패킷 정보만을 모니터링 한다는 제약이 있다. 또한, 해당 종단점에서의 모니터링 소프웨어 동작으로 인한 부하는 단말의 성능을 감소시키게 된다.[3]

더미 허브를 사용하거나 스위치의 포트를 미러링하는 방법은 네트워크 장비들 사이(방화벽과 라우터)에 더미 허브나 스위치를 삽입하여 미러링 포트를 통해 침입 탐지 시스템과 연결하여 트래픽을 감시하는 방법이다. 포트 미러링이란 주로 스위치에서 사용되는 트래픽 포워딩(Traffic Forwording) 기술로 스위치상의 특정 포트를 모니터 포트로 내보내는 방법이다. 이러한 방법은 에러나 VLAN(Virtual LAN)정보에 대해 필터링하는 스위치 기능에 의해 해당 패킷을 모니터 할 수 없다는 단점이 있고, 또한 고속 이더넷(Fast Ethernet)용 미러 포트는 링크상에서 전 이중 방식 모드일 경우 양방향의 트래픽을 미러링 포트로 복사해야 하므로 완전한 모니터링이 힘들게 된다. 특히 트래픽이 많을 때는 스위치의 성능에 영향을 주기도 한다.[2]

수동적 TAP 장비를 사용하는 방법은 1 계층인 물리계층(Physical Layer)에서 포트 미러링을 수행하게 하는 것이다. 네트워크 장비들 사이(스위치와 라우터, 스위치와 서버)에 TAP 을 삽입하여 이 TAP 의 미러링 포트에 모니터링 장비를 연결하여 트래픽을 감시하는 방법이다.



<그림 1. Passive Tap 의 구조>

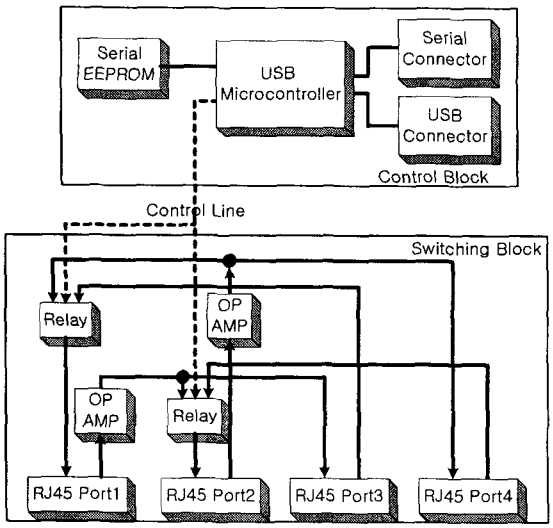
그림 1 은 전형적인 TAP 의 하드웨어 구성을 보여준 그림이다. 이더넷 포트 1 번(RJ45 Port1) 과 2 번에는 원래의 망(실제 망; Real Network)이 연결되고 포트 3 번과 4 번에는 트래픽 분석 장비가 연결된다. 수신된 신호가 두 개로 나누어 져서 생기는 신호 감쇄의 보강을 위해 OP 앰프(Operation Amplifier)를 사용하고 있으며, 전 이중 통신 방식에서도 모든 트래픽을 모니터링할 수 있다. 또한, 물리 계층에서 모니터링하므로 망에 흐르는 모든 트래픽을 직접 모니터 할 수 있다.

본 연구에서는 모니터링 뿐만 아니라 대용량 플러딩 공격에도 대응할 수도 있게 하기 위해 네트웍 연결을 차단하는 방식을 제안하였는데 앞의 모니터링 방법 중 종단점에서 트래픽을 모니터링 하는 방법이나 스위치를 이용하는 방식은 패킷 데이터 손실이나 망 차단 제어가 실질적으로 불가능 한 면이 있다. 그래서 이 두 가지방식이 모두 가능하고 감시 장치와 직접 연결할 수 있는 방식으로 설계하기 위해 물리계층에서 트래픽 흐름을 모니터링하고 침입 탐지를 검출하고 신호를 전달하는 장치와 연결이 가능한 TAP 을 기반으로 목적에 맞는 변경을 시도 하였다.

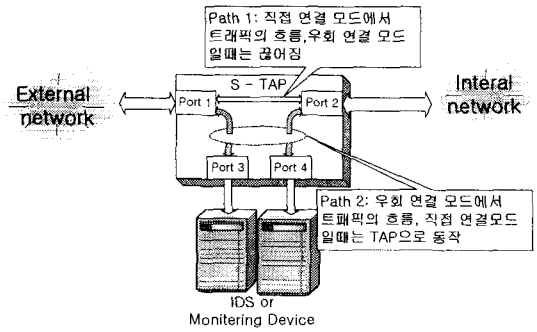
3. Smart-TAP 의 설계

Smart TAP 은 트래픽을 감시하는 IDS 장비에 많이 적용되었던 TAP 의 본래 기능인 모니터링 블록에 IDS 등에서 위험 신호를 받아 연결된 망을 끊을 수 있게 하는 스위칭 블록을 추가한 장치이다. IDS 는 DDoS 나 플러딩 공격과 같은 불필요한 과다 트래픽 발생시 S-TAP 에 차단 신호를 전달 할 수 있다. 이에 대한 세부 설계는 다음과 같다.

그림 2 와 같이 S-TAP 은 크게 호스트 장비에서 제어 정보를 전달 하고 받기 위해 USB(Universal Serial BUS)와 시리얼 라인으로 연결되어있는 컨트롤 블록과 네트워크 라인을 직접 연결하거나 끊는 동작을 하는 스위칭 블록으로 나뉘어져 있다.



<그림 2. Smart - TAP 의 구조>



<그림 3. Smart - TAP 연결 시 트래픽 흐름도>

컨트롤 블록은 USB 장치(USB Target)로서의 동작하기 위한 USB 마이크로 컨트롤러와 펌웨어(Firmware)를 삽입하기 위한 메모리(Serial EEPROM)로 구성되어 있다. 스위칭 블록은 통신을 위한 이더넷 커넥터(RJ45)와 OP 앰프, 릴레이(Relay)로 구성되어 있다. 4 개의 이더넷 커넥터 중 2 개는 실제 트래픽이 흐르는 망과 연결되어 각 커넥터는 전 이중 통신을 그대로 수행하고 있다. 나머지 두 개의 커넥터에서는 각각 한 방향씩에 대한 트래픽을 모니터링하여 네트워크의 이상을 감지하고 판단할 수 있는 장치(IDS, 네트워크 분석 장비)에 전달 하도록 해준다. 그러므로 감시 장치는 최소 2 개의 네트워크 인터페이스를 갖춰야만 오가는 모든 트래픽을 확인 할 수 있다. 릴레이는 망을 연결하거나 분리해주는 역할을 하는데 컨트롤 신호에 의해 물리적으로 두개의 라인 중 하나의 라인과 연결시켜준다.

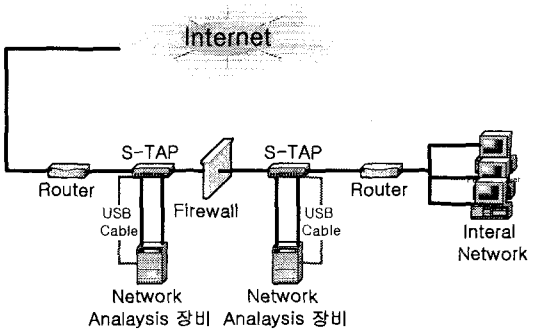
S-TAP 에는 외부 장비의 제어 신호에 따라 직접 연결 모드와 우회 연결 모드 등 두 가지 방식으로 동작한다.

직접 연결 모드는 정상적인 망 연결을 원할 경우나 S-TAP 장치 및 감시 장비의 전원 이상 문제 등이 발생했을 경우에도 정상적인 네트워크 서비스를 지속하기 위한 모드이다. 직접 연결은 1, 2 번 포트 사이에 트래픽이 흐르고, 3, 4 번 포트에도 모니터링 된 트래픽이 흐르는 형태가 된다.

우회 연결 모드는 공격에 대응하기 위해 망의 연결을 외부 장비에서 USB 나 시리얼라인을 통해 끊도록 하는 신호를 전달 받았을 때 동작한다. 이때는 그림 3 에서와 같이 1, 2 포트사이의 망 연결이 끊어지고 대신 1, 3 포트 사이와 2, 4 포트 사이만이 연결된다.

4. 제어 실험 및 실제 적용 방법

S-TAP 의 적용 실험을 위해 그림 4 와 같이 실제와 상당히 흡사한 네트워크 모형을 구성하였다.

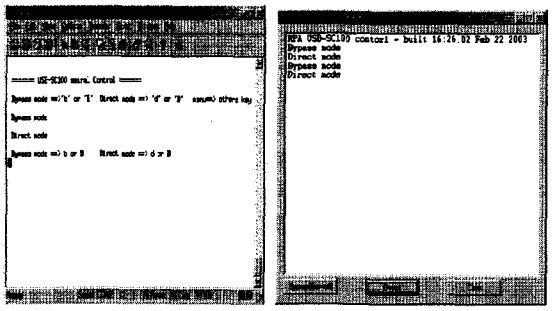


<그림 4. S - TAP 과 네트워크 트래픽 분석 장비와의 연동시의 네트워크 구성>

S-TAP 의 두 개의 포트는 기존 망 구성을 유지하는데 사용되고, 다른 두개의 포트는 양방향 트래픽을 모니터링하기 위해 네트워크 분석 장비에 연결되어 있으며, S-TAP 의 제어를 위한 USB 와 시리얼 라인이 네트워크 분석 장비에 연결되어 있다.

감시 시스템에서 시리얼 터미널과 S-TAP 어플리케이션을 이용하여 S-TAP 을 제어 할 수 있게 제어 프

로그램이 작성하였다.(그림 5)



<그림 5. 시리얼 터미널(왼쪽) 과 USB(오른쪽) 어플리케이션을 통한 S-TAP 의 제어 실험>

실제 제어 신호에 의해 망의 연결과 차단이 정상적으로 이루어 졌으며, 전원 차단 실험에서도 망의 연결에 문제가 없었다. 그러나 S-TAP 에서는 기존 네트워크 망의 연결을 끊고 다른 네트워크 망으로 스위칭 될 때 릴레이가 사용되므로, 외부의 신호에 의해 물리적으로 두 개의 선 중 하나를 선택하여 연결하게 되어 스위칭되는 짧은 시간 동안이나마 망이 단절된 상태가 된다.

문제가 되는 스위칭 시간 동안에 발생하는 패킷의 분실율은 다음과 같이 계산 할 수 있다. 릴레이의 최대 스위칭 시간(T), 라인의 최대 대역폭(B), 패킷 크기(P)라 하면 이에 대한 최대 분실된 패킷 수(L)는 다음과 같다.

$$L = \left[\frac{1}{10^6 B} * \frac{8P}{T} \right] + 1 \quad \text{.....수식(1)}$$

100Mbps 이더넷 망에서 64Byte 크기의 패킷들이 수신된다고 가정할 때 일반적인 릴레이의 최대 스위칭 시간이 4mS 이므로, 스위칭에 의해 분실되는 패킷 수 L = 2 개가 된다. 즉, 릴레이의 스위칭에 대한 분실되는 패킷의 수는 아주 적은 편이므로 망의 정상 복원에도 큰 손실은 없다고 할 수 있다.

5. 결론 및 향후 연구

본 논문에서는 기존의 네트워크 트래픽을 모니터링을 하기 위한 TAP 장치의 기본 구조를 이용하여 기존의 TAP 의 기능을 유지하면서, 네트워크 모니터링 장비들에 의해 DDoS 공격 같은 네트워크 장애가 감지되면 모니터링 장비들의 컨트롤에 의해 내부 네트워크를 물리적으로 외부 네트워크와 단절시키거나 다른 네트워크와 연결하여 내부 네트워크를 보호할 수 있는 S-TAP 의 설계에 대해 서술하였다. 이는 기본 설계 방식을 적용하면 광(Optical) 네트워크를 기반으로 하고 있는 곳에서도 쉽게 응용할 수 있어 상위 고속망에도 적용할 수 있다.

향후 현재 발생하고 있는 약간의 패킷 손실을 무손실화 해야 할 필요가 있으며 다양한 제어 방식의 개발 등 지능화에 초점을 맞춰 개선해야 할 것이다.

참고문헌

[1] L. Garber, "Denial-of-Service Attack Rip the Internet", Computer , pp. 1-5, April , 2000

[2] Anita K. Jones, Robert S. Sielken, "Computer System Intrusion Detection: A Survey", February, 2000

[3] Agilent Technologies, "Enterprise LAN Monitoring and Analysis", 2000

[4] 임채훈, 강명희, "인터넷 보안: 가상사설망, 방화벽 그리고 침입 탐지 시스템", 한국통신학회 학술지 기고문, 2000

[6] Eugene H. Spafford "The Internet Worm Program: An Analysis: Purdue Technical Report CSD-TR-823, 1988

[7] CERT/CC, "Advicory CA-2003-04 MS-SQL Sever Worm" http://www.cert.org/, 2003