방화벽에서의 가상 다중세그먼트 구성 기법의 설계 및 구현*

이한웅°, 이승원, 조유근
서울대학교 컴퓨터공학과

Design and Implementation of Virtual Multi-Segment Firewall System

Hanwung Yi Seungwon Lee Yookun Cho
Dept. of Computer Engineering, Seoul National University

요 약

가상 다중 세그먼트(Virtual Multi-Segment)란 하나의 LAN이 라우터나 방화벽을 사용하지 않고 가상적으로 여러 개의 세그먼트로 나뉘어진 것을 의미한다. 일반적으로 같은 LAN에 속한 호스트들일지라도 다양한 보안 정책을 가지게 되는데 그 결과로 우회 경로 공격(bypass path attack)이 가능해지고 계층적(Hierarchical) 방화벽 시스템을 구성하여 다른 보안 정책을 가진 세그먼트마다 방화벽을 구축하고 있는데 이 방식은 방화벽을 여러 개 설치해야 하는 문제가 있다. 이런 문제를 해결하기 위해 본 논문에서 방화벽을 통해 지나오는 각 연결에 대해서 회선체인을 구성하는 기법을 이용하여 가상적인 다중 세그먼트를 구성한다 회선체인구성을 효과적으로 수행하기 위해 Thumbprint 기법을 사용하는데 이 기법은 동일한 시간대에 모든 회선이 갖는 내용에 대한 요약을 만들어 그 요약들을 가지고 어떤 회선들이 같은 내용을 가지고 있는지를 판단하여 회선체인을 구성하는 기법이다. 본 논문에서는 가상 다중 세그먼트 방화벽을 설계와 구현하였다

1. 개 요

방화벽의 목적은 정당한 권리를 획득하지 않은 사용자가 내부 네트워크의 자원에 접근하려는 시도를 막는 것과 중요한 정보가 허가를 받지 않고 네트워크를 통해 외부로 유출되는 것을 막는 것이다[1]. 방화벽에서 다중 세그먼트(Multi-Segment) 구조란 방화벽 내부에서 소그룹 시스템을 보호하기 위하여 하나 이상의 방화벽을 사용하여 내부 네트워크를 계층적으로 나누는 것을 말한다. 다중 세그먼트 방화벽 시스템은 다른 보안 정책을 가진 세그먼트마다 방화벽을 구축하여야 하는데 이 방식은 방화벽을 여러 개 설치해야 하기 때문에 비용이 많이 든다. 가상 다중세그먼트(Virtual Multi-Segment)란 하나의 LAN이 리우터나 방화벽을 사용하지 않고 가상적으로 여러 개의 세그먼트로 나뉘어진 것을 의미한다 본 논문에서는 기존의 다중 세그먼트 구조의 문제점을 설명하고 하나의 방화벽으로 가상 다중 세그먼트 방화벽을 구성하는 기법의 설계와 구현 내용을 설명한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 가상 다중세그먼트 방화벽의 필요성을 설명하고 3장에서는 가상 다중세그먼트 구성을 위한 회선체인(connection chain)구성 기법들을 설명한다. 4장과 5장은 가상 다중세그먼트 방화벽의 설계 및 구현 내용을 기술한다.

* 본 연구는 과학기술부의 특정연구개발사업인 "Internet을 위한 방화벽 및 네트워크 통신 보호 시스템 개발(과제번호 sw-09-01)"의 지원에 의해 이루어졌다.

2. 가상 다중 세그먼트의 필요성

일반적으로 같은 LAN에 속한 호스트들일지라도 다양한 보안정책을 가지게 된다. 예를 들어 회사의 웹서버나 메일서버 등의 호스트들과 회사 내부정보를 다루는 데이터베이스서버나 회사 기밀정보를 보관하는 파일서버들이 같은 보안 정책을 가질 수는 없다 그림 1에서 호스트 A는 외부 호스트 1,2의 접속만 허락하고 호스트 B, C는 외부 호스트 3,4의 접속만 허락하고 호스트 D는 외부 호스트 5의 접속만

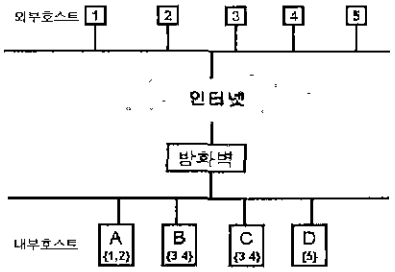

그림 1 가상 다중 세그먼트의 필요성

허락하도록 보안 정책을 만들었을 때 방화벽에서 이러한 보안 정책을 적용시켜도 그 정책들이 제대로 지켜지지 않는다. 왜냐하면 외부 호스트 1의 사용자가 호스트 B로 연결하고 싶을 경우에 사용자는 먼저

호스트 A에 연결하여 방화벽을 통과한 후 호스트 B에 연결할 수 있기 때문이다. 이러한 현상을 우회경로공격(bypass path atlack) 또는 이행적 신뢰(Transitive Trust)이라고 한다[2]

우회경로공격이 가능한 이유는 방화벽에는 일단 방화벽을 통과한 외부 네트워크 사용자에게 보안 정책을 적용시킬 아무런 기능이 없기 때문이다. 우회경로공격을 막기 위한 접근제어방식은 현재까지 두 가지가 있었다 첫 번째 방식은 하나의 LAN에서는 오직 하나의 보안 정책만을 만드는 접근방식이다. 이 방식의 문제점은 웹서버의 경우에는 기업의 광고가 목적이기 때문에 외부의 모든 호스트에서 접속이 가능해야 하는 반면에 데이터베이스서버의 경우에는 내부 호스트들만 접속이 가능해야 하기 때문이다.

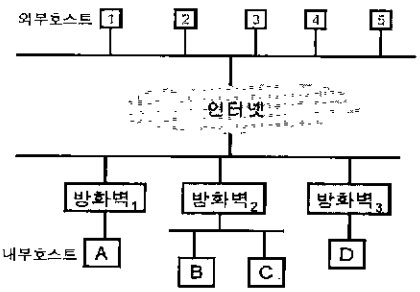

그림 2 기존 우회 경로 공격의 해결방식

두 번째 방식은 그림 2와 같이 계층적 방화벽 시스템을 구성하여 다른 보안 정책을 가진 세그먼트마다 방화벽을 구축하는 것이다. 이 방식은 네트워크 관리자의 관리는 용이해지지만 방화벽을 여러 개 설치해야 하는 비용의 부담이 있다.

3. 가상 다중 세그먼트 구성

3.1. 가상 다중 세그먼트 구성 기법

그림 3은 본 논문에서 제안하는 가상 다중 세그먼트 구성 기법을 보여주고 있다. 호스트 A는 호스트 1과 호스트 2의 접속만을 허락하고 호스트 B는 호스트 3의 접속만을 허용한다고 가정하자. 이때 호스트 1의 사용자가 방화벽을 거쳐서 호스트 A에 접속한 다음 호스트 B에 접속하였을 경우 기존의 방화벽은 아무런 제약도 가할 수가 없었다. 이런 문제를 해결하기 위해 본 논문에서 각 연결에 대해서 회선체인 구성기법을 사용한다. 회선체인이란 사용자가 한 호스트에 로그인한 후 모뎀이나 네트워크 회선을 통해 또 다른 호스트들에 계속해서 로그인을 했을 경우 많은 호스트들이 한 사용자에 의해 telnet이나 rlogin으로 연결되어 사용되게 된다. 이렇게 한 사용자에 의해 telnet이나 rlogin으로 연결된 호스트들이 이룬 체인을 회선체인이라 부른다[3].

3.2. 회선체인

현재 사용되고 있는 네트워크 회선체인을 구성하는 방식은 크게 두 가지로 나눌 수가 있다.

첫 번째 방식은 전체 네트워크에 있는 모든 사용자를 모두 추적할 수 있는 시스템을 만든 후 각 사용자에게 전체 네트워크에서 식별이 가능한 식별자를 주어 모든 사용자의 행동을 기록한 다음에 나중에 회선체인을 구성해야 할 필요가 있을 때 회선체인을 만드는 방법이다. UC Davis에서 개발한 DIDS는 하나의 LAN에서 이러한 방식을 구현한 예이다[4] 이 방식은 항상 전체 네트워크를 감시할 수 있는 시스템이 필요하기 때문에 많은 양의 데이터를 저장하여야 하는 단점을 가지고 있기 때문에 방화벽시스템에 적용하기에는 적당하지가 않다

두 번째로 사용되는 방식은 보통 역추적 방식으로 불린다. 추적시스템이란 추적시스템이 설치된 호스트가 어떤 회선체인에 속해 있을 경우 그 회선체인에서 다음 호스트가 어느 호스트인지를 나타낼 수 있는 능력을 가지고 있는 시스템이다. 따라서 회선체인을 구성하려고 하는 호스트는 자신이 구성하려고 하는 회선체인에 속한 호스트와 통신을 통해 회선체인의 다음 호스트가 이디인지를 알아내어 게인이 구성된 순서와 반대로 역추적 하게 된다. 이 방식으로 구현된 회선체인 구성시스템의 예로는 CIS(Caller Identification System)이 있다[5]

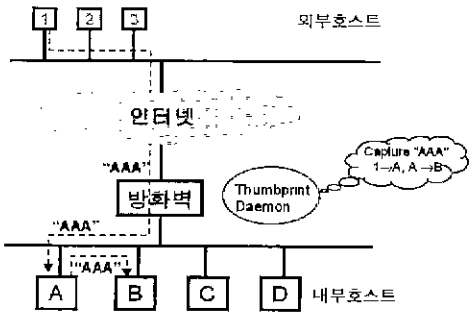

그림 3 가상 다중 세그먼트 구성 기법

이 방식의 가장 큰 문제점은 회선체인의 중간 호스트가 추적시스템을 가지고 있지 않을 경우 회선체인의 구성이 실패한다는 것이다.

이러한 회선체인구성의 문제를 해결하기 위해 본 논문에서 Thumbprint 기법을 사용하여 회선체인을 구성한다. Thumbprint 기법을 이용한 회선체인 구성기법은 동일한 시간에서 볼 때 회선체인을 구성하는 어떤 회선이든 회선을 지나가는 내용은 모두 동일하다는 사실에 기반을 두고 있다 따라서 회선 체인 구성 시스템이 동일한 시간대에 모든 회선이 갖는 내용에 대한 요약을 만들 수 있다면 그 요약들을 가지고 어떤 회선들이 같은 내용을 가지고 있는지를 판단하여 회선체인을 구성할 수 있게 된다.

본 논문에서 제안한 가상 다중 세그먼트 기법은 다음과 같다.

먼저, 방화벽이 호스트 1에서 호스트 A로 전달되는 문자열의 패턴이 "AAA"임을 Thumbprint데몬에게 알려준다 Thumbprint데몬은 LAN을 감시하여 "AAA" 문자열 패턴을 지닌 연결을 찾아내 회선체인을 구성한다. 회선체인을 구성한 Thumbprint데몬은 회선체인의 마지막 호스트를 방화벽에게 알려주고 방화벽은 마지막 호스트가 호스트 1에게 접속을 허락했는지를 확인한 후 접속이 허가되지 않은 경우에는 접속을 끊도록 한다[6].

4. 방화벽 시스템 설계

4.1. 가상 다중 세그먼트 구성 기능

본 논문에서 제안한 가상 다중 세그먼트 구성 기법은 특정 연결을

지나가는 문자열을 패턴을 기준으로 같은 문자일의 패턴을 가지는 다른 연결을 찾아내어 같은 연결회선을 만들어야 한다. 이렇게 하기 위해서는 방화벽이 다음과 같은 기능을 가지고 있어야 한다.

- 방화벽을 지나가는 특정 연결에 대한 문자열의 패턴을 알아낼 수 있는 기능
- 내부 네트워크를 감시하여 위의 문자열 패턴과 같은 문자열 패턴을 가지는 다른 연결이 있는지를 알아내는 기능

4.2. 문자열 패턴 비교의 문제점

- 시간의 불일치(clock skew)

방화벽과 내부 네트워크를 감시하는 호스트가 동일한 호스트가 아닐 수 있기 때문에 방화벽과 내부 네트워크를 감시하는 호스트는 똑같은 시간에 감시를 시작하고 똑같은 시간에 감시를 끝낼 수 없다. 즉, 한쪽에서는 n분에 지나간 문자열 패턴을 생성하는데 다른 쪽에서는 n+1분에 지나간 문자열 패턴을 생성하여 두 문자열 패턴을 비교함으로써 에러를 발생시킬 수 있다

- 전달 지연(propagation delays)

같은 회선체인에 속한 연결들이라 할지라도 다른 지역에 호스트가 존재할 경우 전달 지연 때문에 같은 시간동안에는 약간 다른 문자열 패턴을 보이게 된다 개발한 방화벽에서 가장 문제가 된 것은 네트워크 자체의 전달 지연보다는 회선체인에 속한 부하가 많은 호스트이다. 부하가 많은 호스트는 자신이 전달받은 문자열을 전달하는데 길게는 몇 초를 지연시키는 경우도 있었다.

- 문자열 상실(Loss of characters)

내부 네트워크의 감시는 연결에 참여하여 전달되는 문자열을 감시하는 것이 아니라 수동적인 연결 감시이기 때문에 TCP에서 담당하는 흐름제어나 에러처리부분에 접근할 수가 없다. 따라서 버퍼 오버플로우로 인해 생기는 문자열 상실이 일어날 수 있다.

4.3. 제안된 문자열 패턴 비교법

방화벽을 통과한 문자열 패턴을 기준으로 하여 내부 네트워크 연결의 문자열 패턴이 기준 문자열 패턴(방화벽을 통과한 문자열 패턴)에 비해 얼마나 차이가 나는 가를 판단하여 일정한 값 이하로 차이가 날 경우에는 같은 회선체인에 속하는 연결로 간주하기로 하였다.

본 방화벽은 사용자의 키보드로 입력해 클라이언트에서 서버 방향으로 방화벽을 통과한 문자열을 각 문자별로 통과한 문자수를 계산하여 기준 문자열 패턴으로 정한 후 같은 시간동안 내부 네트워크 연결들을 클라이언트에서 서버방향으로 통과한 문자열 패턴들도 동일한 방법으로 생성한다. 그런 다음 두 문자열 패턴의 편차를 계산하여 편차가 0.2이하인 연결들은 같은 회선체인에 속한 연결들로 간주하였다.

5. 방화벽 시스템 구현

5.1. 구현 환경

본 논문에서 개발한 가상 다중 세그먼트 방화벽은 범용 운영체제인 FreeBSD 2.2.2-RELEASE를 기반으로 C언어와 Perl을 사용하여 구현하였다. 개발한 방화벽이 IP 패킷 라우팅기능을 수행하여야 하기 때문에 네트워크 인터페이스 카드는 2개 이상이 플랫폼에 장착되어 있어야 한다. 본 논문에서는 펜티엄 PC에 2개의 네트워크 인터페이스 카드를 장착하여 가상 다중 세그먼트 통합 방화벽을 구현하였다.

5.2. 구현 내용

본 논문에서 개발한 가상 다중 세그먼트 방화벽은 규칙에 따라 IP 패킷을 처리하는 필터 모듈, 내부 네트워크와 외부 네트워크를 감시하고 회선체인을 구성하는 Thumbprint데몬, 커널 영역의 로그정보를 읽어서 파일로 저장하는 로그데몬, 필터 모듈에 규칙을 전달하고 필터 모듈의 정보를 읽어들이는 관리자 인터페이스로 구성된다.

Thumbprint 데몬은 libpcap-1.7이라는 라이브러리를 이용하여 구현하였다. libpcap은 패킷을 네트워크 인터페이스로부터 획득하여 사용자가 접근할 수 있는 사용자 메모리에 복사한 다음 사용자가 지정한 함수를 메모리에 복사된 패킷에 수행하도록 한다[7]. Thumbprint 데몬은 libpcap을 이용하여 패킷을 획득한 다음 그 패킷을 회선체인을 구성하는 함수에 적용시켜 회선체인을 구성하도록 하였다. 개발된 방화벽의 필터 모듈이 Thumbprint 데몬에게 시그널로 알려주면 Thumbprint 데몬이 회선체인을 구성하도록 구현되었다

6.결론

본 논문은 방화벽에서 회선 체인 구성 기법을 이용하여 가상 다중 세그먼트를 구성하는 방법을 제안하고 구현한 내용을 기술하였다. 개발한 방화벽은 로컬 네트워크에서 서로 다른 보안 정책을 가진 세그먼트마다 방화벽을 구축하여 하는 다중 세그먼트 구조 방화벽 시스템의 문제점을 하나의 방화벽에서 기상적으로 다중 세그먼트를 구성하는 방법으로 해결하였다.

참고문헌

[1]Marcus J. Ranum, "Thinking About Firewall, Proceeding of Second International Conference on System and Network Security and Management", pp. 1-14, 1993

[2]William R Cheswick and Steven M Bellovin, "Firewall and Internet Security", pp51-83, Addison-Wesley, 1994

[3] Stuart Staniford-Chen and L. Todd Heberlein, "Holding Intruders Accountable on the Internet", Proceeding of 1995 IEEE Symposium on Security and Privacy, pp 39-49, May 1995.

[4] S. Snapp, "DIDS(distributed intrusion detection system) - motivation, architecture, and an early prototype", Proceeding of 14th National Computer Security Conference, 1991.

[5] H T Jung, "Caller identification system in the internet environment", Proceeding of 4th USENIX Security Symposium, 1993

[6] 이승원, 조유근, "이행적 신뢰 방지의 방지를 위한 방화벽시스템의 설계 및 구현", 한국정보과학회 '96 가을학술발표논문집(B), pp. 1435-1438, 1996

[7] S. McCanne and V. Jacobson, "The BSD packet filter: A new architecture for user-level packet capture", Proceeding of USENIX '93 Winter Conference, pp259-269