RBAC정책기반의 Rule-DB를 이용한 네트워크 침입차단 시스템 설계 및 구현

박명호O,육상조,이극
한남대학교 컴퓨터공학과
{mhparkO, youksj, leegeuk}@kiss.or.kr

A Design and Implement of Network Intrusion Protection System using Rule based DB and RBAC Policy

Myung-Ho ParkO,Sang-Jo Youk,Geuk Lee
Dept. of Computer Engineering, Hannam University

요 약

RBAC(Role-Base Access Control)은 호스트상의 유저(User)들에게 Role을 적용하여 호스트를 분산 관리하는 방식이다. 본 논문에서는 RBAC방식을 응용하여 Role을 네트워크의 호스트에 적용해서 네트워크 자원 사용에 제한을 두는 침입차단 방식을 제안한다. 그리고 Rule의 적용을 메뉴화하여 선택함으로 Rule적용의 편이성에 기여하는 불법적이고 불필요한 사용을 방어할 수 있는 네트워크 침입차단 시스템을 설계 및 구현을 한다.

1. 서 론

RBAC정책의 목적은 컴퓨팅 자원 및 통신 정보자원 등을 부당한 사용자로부터 사용되거나, 수정, 노출, 파괴와 같은 비합법적인 행위로부터 보호하는데 있다. 또한 침입차단 시스템은 네트워크 서버에 위치하고 있는 일련의 연관된 프로그램들로서, 다른 네트워크의 사용자들로부터 네트웍의 자원들을 보호해주는 것이다.

기본적으로 방화벽은 라우터 프로그램과 일접하게 동작함으로써, 모든 네트웍 패킷들을 그들의 수신처로 전달할 것인지를 결정하기 위해 검사하고, 여과한다. 또한 방화벽은 워크스테이션 사용자 대신 네트웍에 요청을 해주는 Proxy 서버의 기능을 아예 포함하거나 또는 함께 상호 협력하여 동작한다.[5] 불법적인 사용자나 호스트를 필터링하기 위해 사용되는 방화벽은 현재 일반화되어 기업, 공공단체 에 사용되지만 PC방과 인터넷 카페와 같은 특정목적의 네트웍에서는 사용하지 않는 것이 일반적이다. 그것은 보안업체에서 제공하는 방화벽을 구입하는 것은 비용과 인력이 필요로 하기 때문이다. 무료로 배포되는 방화벽 리눅스기반의 Ipfwadm,Ipchains,Iptables 같은 경우에는 숙달되지 않는 전문가가 아니면 필터링정책을 올바르게 설정하기 어려운 단점을 또한 가지고 있다.

본 논문에서는 보안도구의 비용절감과 유지를 쉽게 하고 호스트상의 사용자에 대한 보안정책 설정을 쉽게 해주는 RBAC기법을 응용한 침입차단시스템을 설계 및 구현한다.

본 논문은 2장 관련연구에서는 RBAC기법과 네트워크 기반 침입차단 시스템의 구성 그리고 RBAC기법 적용 시 자원관리의 효율성에 대하여 알아보고 3장에서는 RBAC기반의 침입차단시스템을 설계를 하고 4장에서는 구현 제시한다. 끝으로 5장에는 결론을 맺는다.

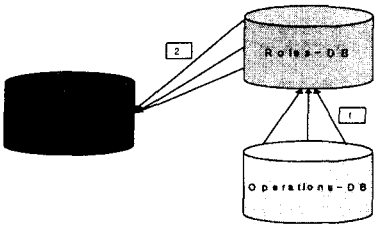
2. 관련연구

2.1 RBAC기법

RBAC(Role-Based Access Control)의 중심적인 개념은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소자원만을 접근할 수 있도록 한다.[3] 이러한 기법은 권한관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다.

RBAC의구성도는 <그림1>과 같다. Operations-DB 안에는 있는 시스템의 데몬 또는 사용자 프로세스 구동, 자원에 대한 사용 또는 작동권한이 정의되어져 있다. Role-DB는 Operations-DB들을 Role별로 그룹화를 시켜놓은 것이다. 마지막으로 User-DB에는 시스템의 각각 User들이 사용하는 Role들을 정의하여

놓은 것이다.



<그림 1> RBAC기법의 구성도

Operations-DB안에는 있는 각각 시스템의 데몬 또는 사용자 프로세스 구동 과 사용에 대한 작동권한이 정의되어져 있는데 <그림1>의 [1]번 과정은 Operation-DB를 조합하여 분류되어진 Role에 포함시키는 과정을 말한다. [2]번 과정은 그렇게 만들어진 Roles-DB를 시스템의 사용자에게 적용을 함으로서 시스템의 사용자들은 정해준 Role에 따라 역할을 수행할 수 있는 권한을 가지게 된다. 이 과정을 통해 사용자의 권한관리를 단순화하고 유저들 에게 관리권한을 분산시킴으로 하나의 관리자에게 만 부과되는 관리역할을 분할 할 수 있다.

2.2 침입차단시스템의 정의

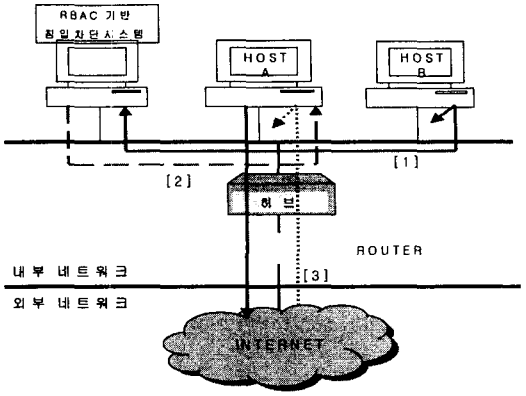
외부로부터 내부망을 보호하기 위한 네트웍 구성요소 중의 하나 외부의 불법 침입으로부터 내부의 정보자산을 보호 외부로부터 유해정보 유입을 차단하기 위한 정책과 이를 지원하는 하드웨어 및 소프트웨어를 말한다. 내부 네트워크를 보호하기 위해 외부에서의 불법적인 트래픽 유입을 막고, 허가되고 인증된 트래픽만을 허용하려는 적극적인 방어 대책이다.[5] 침입차단시스템의 목적은 인터넷을 통한 불법 사용자 및 해커의 침입으로 인한 정보의 손실, 파괴, 변조 등의 피해 발생 인터넷의 확장으로 부가되는 각종 서비스로 인한 기업의 전산 의존도 증가 내부 자원의 안전한 외부 제공 및 외부 불법침입의 차단이다.

침입차단시스템은 일반적으로 라우터의 후반부에 위치하여 라우터에 포워딩하여 오는 패킷을 분석후 필터룰과 비교하여 허용 또는 거부한다.

3. RBAC기반의 침입차단 시스템 설계

3.1 시스템의 동작과정

본 논문은 RBAC기반 침입차단 시스템의 동작과정을 [그림 3]과 같이 구성하였다. 동작과정은 먼저 네트워크 인터페이스 카드를 Promiscous모드로 변경하여 자신의 네트워크 지나가는 패킷을 수집한다.



<그림 2> RBAC 침입차단시스템 동작구조도

<그림2>는 더미 허브환경에서의 RBAC기반 네트워크 침입차단시스템의 동작과정이다 [1]번과정은 Host A가 유해한 사이트, 프로그램에 접속을 요청하거나 원격지에 있는 백도어 클라이언트 프로그램에 응답을 하기 위해 패킷을 전송하는 과정이다. 전송되는 패킷은 허브 및 라우터를 통해 원격지로 향한다. 이와 동시에 침입차단 시스템이 구동되고 있는 시스템과 HOST B에도 패킷이 전달되며 Host B는 자신의 목적지 mac 주소가 자신의 것이 아니므로 이를 버리게 되는 반면, 침입차단시스템이 구동되고 있는 호스트의 네트워크 인터페이스카드는 promiscuous 모드로 설정되어 있기 때문에 다른 호스트의 패킷도 받아들이게 된다. [2]번과정은 RBAC기반 네트워크 침입차단 시스템이 받아들인 패킷을 설정된 Role에 의해 검사를 하게 되고 Role에 어긋나는 접속인 경우 ICMP Protocol unreachable message를 HOST A에 전송하게 되는 과정을 말한다. HOST A는 이 메세지를 받고 접속을 요청한 호스트가 문제가 있다는 것으로 인지하고 이를 해당 응용프로그램에게 통지하게 된다. [3]번과정에서는 이후 HOST A가 접속을 요청했던 호스트로부터 오는 패킷은 HOST A에서 이미 처리가 되었으므로 무시하게 되는 과정을 말한다.

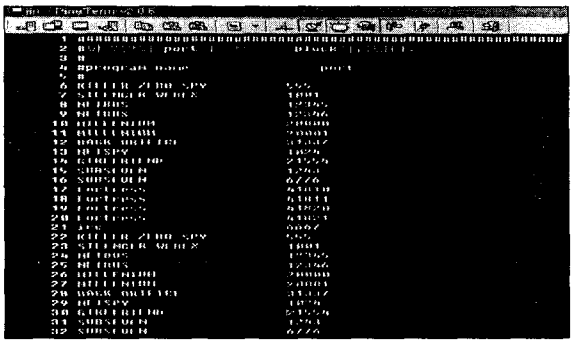
또한 네트워크환경이 스위치환경일 경우 대비하여 RBAC기반의 침입차단 시스템은 arp-spoofing기능 사용하여 조작된 ARP-Redirect패킷을 에 전달하여 라우터로 가는 패킷을 자신의 호스트로 포워딩하게 되어 RBAC기반 네트워크 침입차단 시스템의 Role 설정에 의해 검사를 한 후 Role설정에 어긋나는 접속인 경우 ICMP Protocol unreachable message를 HostB에게 보내어 정상적인 응답으로 처리하게 한다. 더미환경과 다른 점은 패킷이 외부로 나가는 것이 아니므로 외부에서 Host B에 대해 응답이 오지 않는다는 것이다. 이렇게 함으로 RBAC기반의 침입차단 시스템에서는 내 네트워크 안에 있는 호스트들을 설정해 놓은 Role에 따라 네트워크 사용을 제한하고 권한을 부여할 수 있게 된다.

3.2 로깅 및 스케쥴링

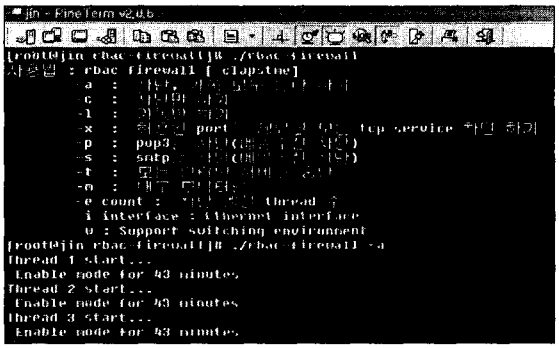
로깅을 위한 로그는 3가지로 분류한다, 유해사이트, 도메인을 차단한 경우에 정보를 저장하는 site-log, 허용되지 않은 네트워크 프로그램 차단 정보를 저장하는 program-log, 백도어 차단 로그인 backdoor-log로 나누어져 있다. 필터링모듈에서 RBAC를 적용하여 필터링한 Log정보는 관리자에게 호스트들의 네트워크자원 현황을 파악하기 쉽게 해준다.

4. RBAC기반의 침입차단 시스템 구현

RBAC기반의 침입차단시스템은 Linux 기반으로 구현되었다. 아래 그림은 RBAC기반의 침입차단시스템의 구현화면을 보여주고 있다. 파일안에 관리대상IP,관리포트 적용 서브넷범위 등을 명세하고 파싱모듈이 파일의 내용을 파싱하여 패킷을 모니터링후 캡쳐해 RBAC정책에 따라 필터링해낸다. 아래 <그림3>,<그림4>는 패킷필터링 검사항목에 대한 정의와 RBAC기반 침입차단시스템의 구동화면이다.



<그림 3> RBAC기반의 침입차단시스템의 관리포트 정보테이블



<그림 4> RBAC기반의 침입차단시스템 메뉴 및 구동화면

5. 결 론

본 논문에서는 RBAC개념은 사용자(User)에 Role을 적용한 기존의 RBAC방식이 아니라 Role을 네트웍상의 호스트에 적용하여 각 호스트들을 Role별로 관리하여주는 침입차단시스템을 설계 및 구현하였다.

RBAC기반의 침입차단시스템의 장점은 라우터에 설치는 하는 침입차단 시스템의 형태는 물론이고 또한 네트워크상의 호스트에 설치하여도 침입차단 시스템의 기능을 모두 사용할 수 있다. 또한 Arp-spoofing 기법을 스위칭환경에서 사용해서 스위치환경에서 패킷수집을 가능하게 하는 기능을 포함한다. 또한 RBAC기반으로 한 필터링 기법을 사용함으로서 패킷의 필터링 규칙을 복잡하게 사용자가 설정해 주지 않고 설정된 Role만 Hosts-DB에 적용함으로 효율적인 패킷의 필터링이 가능하다.

적용분야는 호스트별로 네트워크 자원사용을 제한하여 호스트별 네트워크 보안설정이 필요한 회사, 공공기업 PC방등 에 적용될 수 있다.

본 논문에서는 스위칭 환경에서 패킷을 수집하기 위해 Arp-spoofing기법을 사용하였다. 이러한 기법 사용시 네트워크 부하로 작용될 수 있으므로 ARP패킷의 부하를 줄이는 방안 연구가 향후 필요하다.

[참고문헌]

[1] 정진욱 외 2인 "TCP/IP 네트워크" 1999, 도서출판사 진영사

[2] 오석균,김성열 "RBAC보안 시스템에서 보안관계 관리를 위한 관리 도구동작"

[3] 오석균,김성열 리눅스 보안 시스템을 위한 RBAC_Linux 설계 한국산업정보학회 논문지제.4권 4호1999

[5] 이재광,이용준,박성열 "인터넷 방화벽과 네트워크 보안" 1999, 이한출판사

[6] http://www.terms.co.kr "컴퓨터 용어 사전"

국문 : 본 연구는 한국과학재단 지역협력연구센터(R12-2003-004-02003-0")지원으로 수행되었음,

영문 : This work was supported by a grant No.(R12-2003-004-02003-0") from Korea Science & Engineering Foundation"