情報保護學會論文誌
第14券 第6號, 2004. 12

침입방지시스템과 역할기반 보안정책을 이용한 정부기관 정보보호 시스템 설계

안 정 철

한국국방연구원

A Government Agency Environment Protects Information System Design using Intrusion Prevention System and Role-Base Security Policy

Joung Choul Ahn

Korea Institute for Defense Analyses

요 약

기존의 네트워크 방화벽에 대한 연구는 정보에 대한 접근을 최대한 제한하는 거부(Deny)정책과 침입을 감지하는 감지 시스템 중심으로 연구 및 발전되어 왔다.

정부기관은 인트라넷(intranet)이라는 외부 인터넷과의 별도 망을 구축함에 따라 방화벽에 대한 문제점을 해결해 왔으나, 전자정부로의 전환에 따라 정부기관(경찰/군/관공서등)에서는 거부정책과 정보공개 두 가지를 모두 만족시켜야 한다. 즉 상급부서와의 정보교환이나 민간인에 대한 대민 서비스 등을 위하여 부분적인 정보 공유, 네트워크 접속 및 불법접근을 차단하여야 한다. 또한, 현재 많이 문제시되고 있는 내부사용자에 대한 해킹과 Worm에 대한 공격에 대한 방어에 미흡한 점은 새로이 극복해야 하는 문제점으로 대두되고 있다.

따라서 본 연구에서는 정부기관들의 정보공유 및 대민서비스를 위한 "부분공개성" 및 불법 접근에 대한 "거부정책"을 충족시키기 위하여 IPS(Intrusion Prevention System)와 역할기반보안정책(Role-Base Security Policy)을 이용한 정보보호시스템을 제안하고자 한다.

ABSTRACT

The survey of network firewall system has been focused on the deny policy that protects information from the unlicensed and the intrusion detection system.

Government has solved several firewall problems as building the intranet separated from the intranet. However, the new firewall system would been satisfied both the denialpolicy and information share with the public, according as government recently emphasizes electronic service.

Namely, it has to provide the functions such as the information exchange among divisions, partial share of information with the public, network connection and the interception of illegal access.Also, it considers the solution that protects system from hacking by inner user and damage of virus such as Worm.

This paper suggests the protects information system using the intrusion prevention system and role-based security policy to support the partial opennessand the security that satisfied information share among governments and public service.

Keywords : *PKI, PMI, Certificate Verification, PKC, AC*

접수일 : 2004년 8월 24일 ; 채택일 : 2004년 11월 26일

† 주저자 : killban@empal.com

Ⅰ. 서 론

기존의 정부기관은 폐쇄망에서 업무를 실시하였으나 전자정부의 대국민 서비스를 시점으로 관련부서에 대한 정보공유 및 접속권한이 부여되어야 하며, 시민들을 위한 정보의 부분적인 개방이 필요하다.

현재 정부기관의 정보보호시스템은 불법 공격에 대한 방어를 중심으로 구축되어 있다. 그러나 기존의 네트워크 방화벽은 Worm과 같은 새로운 공격과 내부사용자에 대한 방어대책은 미흡한 것이 현실이다.[7-10]

그림 1은 기존의 정부기관의 정보보호 시스템을 나타내는 것으로서, 현재의 네트워크방화벽 시스템은 [a]와 같이 방화벽을 중심으로 구축되어 있으며, 일부는 [b]와 같이 공격에 대한 탐지가 가능하도록 추가 개량된 경우가 대다수이다.[7-10]

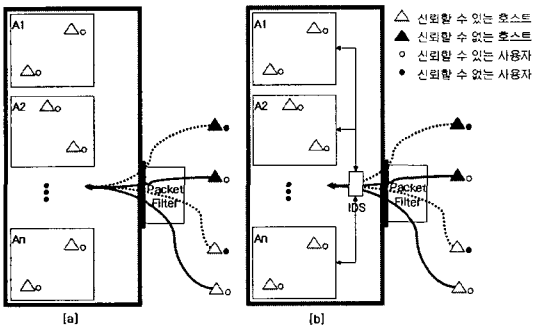


그림 1. 기존의 방화벽시스템 구조

따라서 본 논문에서는 IPS(Intrusion Prevention System)와 역할기반 보안정책을 이용한 정부기관에서 요구되는 공개성을 충족하고, 정부기관의 자료에 대한 보안성을 지키며, 또한 보다 추상적인 방법으로 정책을 표현 할 수 있는 방법을 제안하였다.

본 논문에서는 2장에서 대표적인 네트워크 방화벽 및 역할기반 보안정책에 대하여 살펴보고, 3장에서 정부기관 환경의 특징을 살펴본 뒤, 그 특징을 충족시킬 수 있도록 역할기반 보안 정책을 이용한 네트워크방화벽 시스템 모델을 제안한다. 마지막장에서는 결론 및 향후 연구에 대하여 논하였다.

Ⅱ. 네트워크방화벽 시스템 및 관련연구

네트워크 보안은 내/외부 네트워크에 의한 영향을 받지 않아야 한다. 네트워크 보안수준은 가장 약한 링크의 보안수준이라는 것을 기억하여야 한다. 또한, 모든 기업 및 정부기관은 보안 정책을 가지고 있어야 하고 외부 네트워크에 대한 연결을 그 정책에 따라야만 한다. 보통 이것은 어떤 종류든 정보보호 체계을 통해서만 가능하다.

정보보호 체계는 기밀정보가 나가는 것과, 공격자가 들어오는 것을 차단하는 데 도움을 준다.

네트워크들 사이의 통신에 대한 자세한 통계를 제공할 수 있으며(누가 어떤 서비스를, 얼마나 자주 쓰는지와, 성능상의 병목지점을 보여주는 등) 통신에 대한 로깅과 감사 정보를 제공할 수 있으며, 로그를 분석하면 공격자를 탐지하고 알람을 울리는 데 사용할 수 있다.

그러나, 강력한 정보보호 체계가 곧 더 이상 내부 호스트 보안이 필요 없음을 의미하는 것은 아니다. 대부분의 성공적인 공격은 내부자로부터 시작되기 때문이다.

정보보호 체계에서 다루는 기술적 위협의 예로는 IP spoofing, ICMP 폭탄, 위장(masquerading) 및 취약하게 구성된 내부 시스템 접근 등이 있다.

정보보호 체계로 감소되는 위험의 예로는 호기심 많은 또는 악의적인 해커들로부터의 공격, 산업 스파이, 회사 데이타(즉 고객, 근로자 및 회사 데이타)의 우발적 노출 그리고 서비스 거부 공격 등이 있다.

이러한 기술적인 위협으로 인하여 정부기관의 정보보호체계는 은 기본적으로 아래와 같은 특징을 만족하여야 한다.

① 비밀을 요하는 자료의 접근제한
② 업무를 위한 관련부서 및 부처간의 정보공유
③ 대민서비스를 위한 정보접근 허용
④ 네트워크의 안전성 제공
⑤ 내부사용자 공격에 대한 방어등

이러한 특징은 실제로 정보보호시스템 구축시 장비 도입이나 설치에 많은 영향을 주고 있다.

여기서는 현재 나와 있는 네트워크 방화벽의

대표적인 종류인 방화벽(Firewall), IDS(Intrusion Detection System), IPS와 역할기반 보안정책에 대하여 알아보겠다.

2.1 방화벽

방화벽의 원래 의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는 것이다. 이 의미를 인터넷에 적용한다면, 이는 네트워크의 보안 사고나 위협이 더 이상 확대되지 않도록 막고 격리하는 것이라고 할 수 있다. 이는 특히 어떤 기관의 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 적극적인 방어 대책이라고 할 수 있다.

방화벽 시스템의 기본 목표는 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공하는 것이다.

방화벽 은 두 네트워크 사이의 트래픽을 제어하기 위해 특별히 구성된 시스템(또는 시스템들의 네트워크)으로 패킷 필터에서부터, 다중 필터, 전용 프락시 서버, 로깅 컴퓨터, 스위치, 허브, 라우터 및 전용 서버에까지 이를 수 있다.

게이트웨이 즉 배스천 호스트는 어떤 응용프로그램에 대한 접근을 제공하는 안전한 컴퓨터 시스템이다. 나가는 트래픽을 깨끗하게 하고, 들어오는 트래픽을 제한하며 외부로부터 내부 구성을 숨길 수도 있다.

방화벽의 장점으로는 방화벽 기능이 OSI 7 모델에서 제 3, 4계층에서 처리되기 때문에 처리속도가 빠르며, 사용자에게 투명성을 제공한다. 또한 기존에 사용하고 있는 응용 서비스 및 새로운 서비스에 대해서 쉽게 연동할 수 있는 유연성이 있다.

그러나 방화벽의 문제점이 드러나고 있다. 그것은 TCP/IP 프로토콜의 구조적인 문제 때문에 TCP/IP 패킷의 헤더는 쉽게 조작 가능하다. 따라서 외부침입자가 이러한 패킷의 정보를 조작한다면 내부시스템과 외부시스템이 직접 연결된다. 또한 ftp, mail에 바이러스가 감염된 파일 전송시 잠재적으로 위험한 데이타에 대한 분석이 불가능하며 접속제어 규칙의 개수 및 접속제어 규칙 순서에 따라 방화벽에 부하를 많이 줄 수 있다. 또한 다른 방식에 비해서 강력한 logging 및 사용자 인증 기능을 제공하지 않는다.

방화벽은 표 1과 같이 아래의 다섯 가지의 종류로 나눌 수 있다.

방화벽의 작동 원리는 크게 패킷 필터링구조와 서킷 레벨 방화벽으로 구분되어 진다.

패킷 필터링은 OSI의 4 레이어에 해당하는 트랜스포트 레이어에서 네트워크 패킷을 감시하는 처음 세대의 방화벽 기술이다. 이것은 패킷의 방향성과 패킷의 IP나 TCP 헤더에 있는 정보를 보고, 정해진 규칙에 의하여 허락한다.

서킷 레벨 방화벽은 1세대 방화벽 기술로서 상호 트랜스포트 레이어간에 연결에 대한 요청이나

표 1. 방화벽의 종류

종 류	설 명
Packet Filtering 방식의 방화벽 시스템	패킷의 정보를 분석하여 미리 정해둔 규칙에 따라 필터링
Circuit Level 방화벽 시스템	중계를 담당하는 시스템이 있어서 외부 네트워크와 통신을 위해서는 그 시스템에 접속을 의뢰하고 중계 시스템이 외부 네트워크에 접속
Application Level의 방화벽 시스템	Application Proxy를 두고 Session성립 시, 해당하는 Service별 Application Daemon이 인증작업을 하고 인가된 Session에 한해 Service를 허용
앞에서 언급한 방식들을 혼재한 Hybrid 방식의 방화벽 시스템	앞에서 설명한 Firewall 유형들의 단점을 보완하면서 다단계의 인증작업을 수행
앞의 여러 방화벽의 문제점의 해결을 위해 만들어진 Stateful Inspection방식	스테이트풀 인스펙션은 클라이언트/서버 모델을 유지시키면서 모든 어플리케이션층의 전후 상황에 대한 문맥 데이타를 제공함으로서 이전의 세 가지 접근(패킷 필터링과 어플리케이션 게이트웨이 및 하이브리드방식)의 한계를 극복

데이타 패킷에 대한 인증을 해주는 기능을 가지고 있다. 따라서 서킷 레벨 방화벽은 인가된 연결 설정인가를 조사하여 이 과정이 끝나기 전에는 데이터 패킷의 전송이 이루어지지 않도록 하는 것이다.

방화벽은 인가된 연결테이블을 가지고 있으므로 패킷이 이 테이블에 있는 정보를 가지고 있을 때에만 전송을 허락한다. 그리고 이 연결이 종료되면 테이블에서 삭제한다.[12-13]

그림 2는 보편적으로 많이 설치 되어있는 방화벽 중 패킷 필터에 대한 것이다.

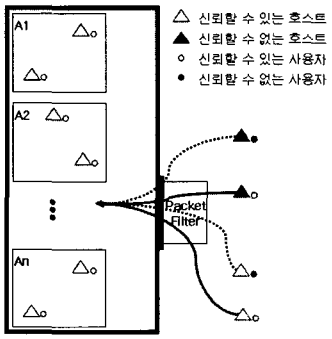


그림 2. 패킷필터 방화벽

방화벽은 관계된 네트워크 내에서 어떤 포트를 막고 어떤 포트를 개방할 것인지를 효과적으로 결정할 뿐이다. 즉, 특정 서비스 시스템이 적절히 구동되기 위해 방화벽은 포트를 개방해야만 한다. 그러나 이러한 개방된 포트는 해커들의 공격을 허락하는 것과 마찬가지이다. 따라서, 열려져 있는 포트들은 해커들이 서버 안으로 들어가고 침입할 수 있게 하는 연결통로 사용된다. 가장 대표적인 예가 웹서버에서 이용되고 항상 열려있는 80번(HTTP 프로토콜) 포트이다.

공격자는 별 어려움 없이 방화벽을 통해 웹서버로 HTTP 메시지를 보낼 수 있고, 그 서버의 약점을 노출시킬 수 있다. HTTP 메시지는 이러한 여러 약점들을 악용할 수 있고 마침내 침입자는 웹서버로 액세스할 수 있는 권한을 가지게 되는 연속적인 이벤트를 야기하게 된다.[15-16]

2.2 침입탐지시스템(Intrusion Detection System)

침입탐지시스템은 침입 즉 자원의 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability) 등을 파괴하기 위한 일련의 시도들을 탐지하기 위한 보안 시스템이다.

침입탐지는 크게 두 가지로 양분할 수 있는데, 이상탐지(Anomaly Detection)와 오용탐지(Misuse Detection)로 나뉠 수 있다. 변칙 탐지란 컴퓨터 자원 사용에 있어서의 변칙적인 행위에 기반을 둔 탐지를 뜻하는데, 임의의 사용자가 작업시간외에 작업을 하거나 작업장소가 아닌 원격에서 로그인을 시도하는 등의 일을 말한다. 오용 탐지란 시스템이나 응용프로그램상의 허점(Vulnerability)을 이용하여 공격하는 침입을 사전에 정의된 침입탐지 패턴과 비교하여 침입의 여부를 판단하는 것으로서 정상적인 데몬의 버그를 이용하여 원래의 프로그램 사용에 맞지 않는 결과들을 이끌어 내도록 유도하는 것 등을 말한다. 침입탐지 시스템은 컴퓨터 시스템 및 네트워크에 가해지는 내외부의 침입 행위를 자동으로 탐지하는 보안 시스템이다. 따라서 방화벽을 뚫고 들어오거나 우회하여 침입을 했을 경우, 혹은 방화벽의 제재를 받지 않는 내부의 공격 행위들 그리고 방화벽의 보호를 받지 못하는 시스템에 대해 이루어지는 모든 침입 행위들을 자동으로 탐지하고 방어하는 것을 목표로 하고 있다.

침입탐지시스템은 호스트나 네트워크에 대한 침입을 탐지하여 이를 보호하기 위한 시스템이다. 즉, 정보보호시스템으로서 보안영역은 보호대상이 되는 호스트, 다중호스트, 네트워크 등이 될 수 있다. 이를 '시스템 보안영역'라 부르기로 한다. 시스템 보안영역에서 침입탐지시스템의 역할은 보안위반 분석을 통한 침입탐지 및 대응행동을 수행하는 것이다. 따라서 시스템보안영역에서는 보안위반 분석을 위한 데이터를 수집하는 축약감사데이터 생성, 침입을 탐지하기 위해 수집된 데이터를 분석하는 보안위반 분석, 분석결과 침입이 탐지되었을 때 수행하는 보안감사 대응 등의 보안기능이 요구된다.

정보보호시스템으로서 원활하게 동작하고 시스템보안영역에 대한 보안기능을 제공하기 위해서는 침입탐지시스템의 자체 보안영역에 대한 보안기능이 요구된다. 관리자의 침입탐지시스템으로의 접근을 통제하는 신분확인, 침입탐지관련 정보의 보호를 위한 데이터보호, 보안관련 사건을 기록하는

표 2. IDS 분류

항목	N - IDS	H - IDS
탐지 대상	네트워크를 통과하는 패킷	시스템 내부 사용자들의 활동
설치 단위	네트워크	세그먼트 호스트
기반 기술	패킷 캡처링	프로세스 모니터링
	프로토콜별 패킷 분석	실시간 로그분석
	패킷 조각 모음	TTY모니터링

표 3. IDS 장·단점

장 점	문 제 점
· 신기술의 적용이 빠르다. · 내부자의 의한 해킹도 차단 할 수 있다 · 접속하는 IP에 상관없이 침입 차단 · 시스템 침입에 즉시 대응 · 침투경로까지 추적가능	· 차단기능이 부재 · 패턴매칭/Traffic양에 의한 탐지로 높은 오탐지율 · 숙련된 네트워크 관리자가 필요 · DoS 공격에 대한 대응 방법 없음

보안감사, 보안기능 관리를 위한 보안관리, 보안기능의 보호 등이 포함된다.

IDS는 모니터링의 대상에 따라 표 2와 같이 크게 네트워크 기반 IDS와 호스트 기반 IDS로[11] 나눌 수 있으며, 장단점은 표 3과 같다.

침입 탐지 시스템이 가지는 일반적인 특성들은 크게 기능적인 것과 비기능적인 것의 두 가지로 나눌 수 있다. 기능적인 특성들은 다시, 원시데이타의 근원지가 어디인지, 탐지 분석 방법이 무엇인지, 대응 행동이 어떠한 지의 세 부류로 나누어진다. 원시데이타의 근원지가 어디인지는 호스트 기반 방식(사용자 감사 자료와 시스템 로그 등)과 네트워크 기반 방식(네트워크 패킷과 네트워크 프레임 등)으로 나누어진다. 탐지 분석 방법의 일반적인 분류방법은 오용 기반(misuse-based)과 이상기반(anomaly-based)으로 나눌 수 있다. 오용기반 침입 탐지 방법은 미리 잘못된 행동들을 지정하고 이 행동들이 발생하는지를 검사하는 것으로, 시그너처 분석 방법(signature analysis) 등이 이에 속한다. 이상기반 침입 탐지 방법은 정상적인 경우의 시스템 및 사용자들의 궤적을 기록해 놓고, 이를 벗어나는 행동들을 침입으로 간주하고 탐지하는

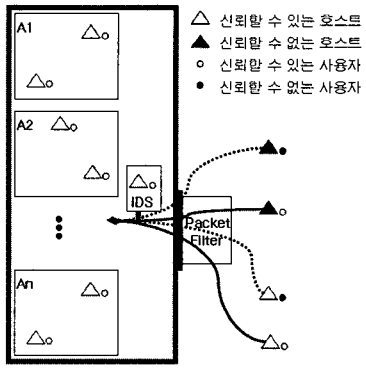


그림 3. IDS를 적용한 정보보호시스템

것으로, 통계적인 방법(statistical approach) 등이 이에 속한다. 침입이 탐지되었을 때의 대응행동은 수동적인 것과 능동적인 것으로 나눌 수 있다. 수동적인 대응방법은 시스템 자체의 수정은 수행하지 않는 반면에, 능동적인 대응방법은 수정이 필요한 경우, 시스템 자체의 수정도 수행한다. 비기능적인 특성이란, 사건 탐지/분석을 수행하는 주기에 관계된 것으로, 준 실시간으로 수행하기, 주기적/배치로 수행하기, 특정 조건에서만 수행하기의 세 가지 부류로 나눌 수 있다.[11]

그림 3은 방화벽에 IDS를 적용한 일반적인 정보보호시스템의 구성을 타나낸 것이다.

IDS의 결점은 실시간으로 공격을 막을 수 없다. IDS는 네트워크에 있는 패킷들을 감지하고 있지만 전송을 차단하지는 않는다. 대개 패킷은 그들의 목적지로 도착하고 IDS에 의해 해석되기 전에 먼저 처리된다. 결과적으로 IDS에 의해 판별되기 전에 공격이 성공하게 된다. 또한, IDS는 알려지지 않은 공격들을 탐지하지 못한다. 어떠한 IDS라도 제품의 데이터베이스 안에 알려진 공격의 서명이 존재할 때만 동작하게 된다.[15-16]

2.3 침입방지시스템(IPS)

침입방지 시스템은 공격 시그니처를 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이뤄지는지를 감시하고, 자동으로 모종의 조치를 취함으로써 해당 활동을 중단시키는 보안 솔루션이다. 이것은 기존의 탐지나 패킷 제어방식보다는 더욱 능동적인 대응 방식으로 최근 많은 분야에서 적용

되거나 도입이 고려되고 있는 방법이다.

방화벽 또는 IDS와 같은 보안제품은 최근에 발생빈도가 증가하는 침입공격에 대하여서는 더 이상 안정성을 확보해주지 못하고 있다. 그중 대표적인 공격이 Worm이다. 2002년 Scalper/Slapper Worm, 2003년 Blaster/Welchia/Sobig/SQL Slammer Worm등의 공격으로 네트워크가 마비가 된 경우가 있었다. 정부기관의 경우에는 업무특성상 일반적인 서버침입으로 인한 정보 유출만 공격이 아니라 업무가 마비되는 것 또한 방어가 되어야 한다. IPS는 이러한 네트워크에 대한 공격까지 방어를 지원한다.

IPS는 수상한 활동을 감시하다가 특정 지정된 서버 등에 대한 비정상적인 행동을 실행하고자 하면 그 즉시 중지시켜버리기 때문에 Worm과 같은 신종 공격에 대하여서도 내구성을 가질 수 있다. 따라서 표 4과 같이 기존 보안장비가 가지는 수동적인 방어 개념의 방화벽이나 IDS와 달리 침입유도 시스템(허니팟)이 지닌 지능적인 기능과 적극적으로 자동 대처하는 능동적인 기능이 합쳐진 개념의 보안 솔루션으로 코드레드, 웜과 같은 신규공격패턴 발생시 보안적용이 어려운 기존 솔루션(방화벽, IDS등)의 대안으로 떠오르고 있는 보안 솔루션이다.[5-6] IPS의 특징과 장점은 표 5와 같으며 현재 IDS에서는 IPS의 기능을 수용하는 과정이 진행중에 있다.

2.4 역할기반 보안정책

분산 시스템 환경의 사용이 증가됨에 따라 관리할 자원과 사용자가 많이 늘어나게 되었다. 이에, 분산 시스템의 보안 측면에서 기존에 사용하

표 4. 기존보안장비와 보안방식

보안장비	방화벽	네트워크 침입탐지시스템	서버침입탐지 시스템
제어방식	패킷의 헤더 정보에 의한 제어	패킷의 헤더정보와 내용검색을 통한 침입탐지 및 차단	패킷검사 및 서버에서의 프로세스 검사를 통한 침입탐지 및 차단
방식	규칙(Rules)	패턴인식	응용방식
위험	높다	보통	낮다
대응	수동적	수동적	수동적

표 5. 침입방지시스템의 특징과 장점

특 징	장 점
· 손실 발생 전 차단시스템 리소스에 대한 접근제한 · 독립된 에이전트 · 기존 보안체계 연계가능 · 관리기능 지원 · 로그정보 export 기능지원 · DDos방어 기술지원 · 세션제한 가능 · SCAN탐지 및 차단	· 서버동작시간 보장 · 시스템노출방지 · 지속적 모니터링 불필요 · 신속한 업데이트 지원 · 중앙화된 보안관리 지원

던 패킷 필터링 규칙 위주의 접근 제어목록(Access Control List)만으로는 정책의 충돌(Confict) 및 보안정책 관리자의 오류(Error)등을 분석하기 어렵고, 정책 구현에 대한 검증이 힘들어졌다. 따라서 분산된 자원의 관리와 보안을 용이하게 하고 대규모 시스템의 관리 책임을 분산시키기 위하여, 공통된 정책을 적용할 대상을 도메인(Domain)단위로 구성하는 역할기반 보안정책 모델[1]에 대한 연구가 진행되었으며, 이 모델에서는 자원 접근을 요청하는 주체(Subject)와 그 요청을 받아들이는 객체(Object)로 구분하고, 주체와 객체 사이에서 주체가 객체에 행할 수 있는 역할(Role)로써 관계가 형성된다. 주체나 객체는 도메인 단위로 구성할 수 있고, 하나의 도메인은 하위 도메인을 포함하여 계층구조를 가질 수 있는 구조이다. 역할은 주체가 객체에 대한 권한 및 의무를 나타낸다. 권한(Right)이란 주체가 객체에 대하여 접근 허가 또는 금지를 의미하고, 의무(Duty)란 주체가 객체에 대하여 꼭 해야 하는 것 또는 절대로 하지 말아야 하는 것을 의미한다. 주체와 객체 사이의 관계를 역할로 표현함으로써, 역할에 적용되는 정책을 재구성 없이 개인에게 역할을 할당 하게나 회수하는 등의 방법으로 정책의 변경이 가능하다.

그러나 역할기반 보안정책은 모든 사용자가 신뢰할수 있다는 전제에서 연구되어 있다는 문제점을 가지고 있다.[1]

Ⅲ. 역할기반 보안정책을 이용한 정부기관 정보보호시스템

본 논문에서는 정부기관 네트워크의 특성을 살

펴보고, 정부기관에서 정보보호시스템을 사용할 경우 정부기관 네트워크 특성을 정보보호시스템에 적용할 수 있도록 역할기반 보안정책을 제안한다. 또한, 정보보호시스템 적용 시 발생할 수 있는 보안정책의 충돌에 대한 문제를 고려하겠다.

3.1 정부기관 환경의 특징

정부기관의 정보보호시스템은 기존 거부방화벽 시스템의 폐쇄성이나, 무분별한 개방성 및 IDS의 침입탐색/감시 기능만으로는 Worm과 같은 신종 공격이나 내부자에 의한 공격에 대한 방어로는 미흡하기 때문에 현재의 네트워크 망에 정보보호시스템을 구축하기에 적합하지 않다.

전자정부는 현재 주민등록 등/초본, 건물대장 등/초본, 토지/임야대장, 소득금액증명 등 여러 분야를 인터넷을 통하여 지원하고 있다. 이러한 업무들은 기존의 폐쇄망에서 운영되어 오던 시스템이 인터넷이라는 공개된 망에 함께 공용되어 사용되는 서비스 들이다. 이러한 서비스 정보가 대량 인터넷에 유출될 시에는 개인 프라이버시 및 범죄에 사용이 될 수 있다.

본 연구에서는 기존 거부환경방화벽의 폐쇄성으로 인한 문제점과, 너무 심한 개방성으로 인한 문제점을 개선하고, 정부기관의 환경에 적합한 보안정책을 반영할 수 있도록 하기 위하여 다음과 같이 정부기관의 환경적 특성을 요약하였다.

첫째, 정부기관의 환경은 시스템 공격으로부터 안전하여야 한다. 시스템 해킹, DDOS공격, Worm형 공격등에 대한 방어 대책이 수립되어 상시 안정적인 정보를 제공해야 한다. 즉, 정부기관의 특성상 비밀 또는 그에 준하는 자료가 존재 하므로, 인가되지 않은 사용자나 패킷 공격 등에 대한 방어책이 수립되어 있어야 하고, 전문 인력이 투입되기 이전에 최소한의 방어 및 격퇴가 가능하여야 한다.

둘째, 정부기관의 네트워크에서는 동시에 여러 가지의 업무(일상 업무, 군 작전, 범인색출 등)가 가능하고, 업무간의 관계 또한 업무 담당자들 간의 관계가 복잡해질 수 있다. 하나의 업무를 처리하기 위하여 각 업무담당자들은 담당업무 정보에 대한 접근권한이 보장되어야 한다. 즉, 업무담당 총괄자는 해당업무의 모든 정보에 대하여 접근이 가능하여야 하고, 각 부분담당자들은 해당 담당업무의 정보만 접근이 가능하여야 한다.

셋째, 정보보호 시스템내의 사용자는 신뢰할 수 있는 사용자와 신뢰할 수 없는 사용자가 공존한다. 즉, 모든 사용자들은 자신이 속한 정보만 접근이 허용되어야 하며, 자신이 담당하지 않는 정보에 대하여서는 접근이 불가능하여야 한다.

넷째, 정보보호시스템에 적용되는 보안정책은 운용중에 변경이 가능하여야 한다. 즉, 업무변경/추가시 추가적인 보안정책을 수정/삽입/삭제 등의 기능이 가능하여야 한다.[7-10]

정부기관의 환경적 특성은 일반기업의 환경적 특성과 유사하다. 그러나 정부는 시민 개개인의 신상정보 및 재산등의 정보를 실시간 지원함에 따라 자료의 중요성 및 제공정보의 중요도가 일반기업과는 비교를 할 수 없을 정도로 .보호가 되어야 한다.

3.2 현 정부기관 전산망 구조

정부기관 전산망 및 시스템관리자의 대표적인 문제점은 일반적으로 나타나는 전산망 및 관리자들의 문제점과 유사하다. 일반적인 문제점을 몇 가지 분석해 보면 아래와 같다.

가. 서버는 UNIX 및 Windows2000를 중심으로 구축되어 있으나 일부의 시스템은 잘못된 설정(초기 설치시 기본설정)을 유지하고 있다.

나. 네트워크를 통한 FTP, TFTP등의 서비스를 아무런 통제 없이 일부를 허용하고 있다. 여기서 TFTP와 같은 서비스는 패스워드를 통합 접근통제를 받지 않기 때문에 망에 연결된 PC에서는 상시 불법적인 절취가 이루어 질수 있다.

다. 네트워크상의 패킷 흐름을 감지하는 시스템은 일부 구현되어 있으나, 대다수가 불법적인 침입이나 탐지에 대하여서는 탐지능력이 제한된다.

라. 시스템 관리자의 대다수가 네트워크 및 해킹관련 보안지식이 미흡하다.

마. 시스템관리자는 시스템이 다운되거나 정기 점검 및 이상이 발생하지 않을 시에는 서버나 네트워크에 관심을 가지지 못하고 타 업무를 수행하는 관계로 자료 절취결과에 대한 확인이 늦어진다. 즉, 로그에 대한 세밀한 분석만이 불법침입 인지가 가능한 관계로 불법 침입자가 자료 절취 후 상당시간이 지난 후에나 확인이 가능하다.

이상이 네트워크 및 시스템운영자의 문제점 중 대표적인 것이다. 정부기관도 일반적으로 나타나는 문제점을 그대로 가지고 있다. 현재 정부기관의 정보보호시스템은 라우터와 서버에서 처리하고 것을 중심으로 IP접근거부 와 사용자 인증을 중심으로 구축되어 있다. 현존 정보보호체계 를 무시하고 접근이 가능한 방법으로는 몇가지가 있다. 그중 가장 보편적인 공격 방법을 소개하면 아래와 같다.

첫째, 외부사용자는 접근 가능한 내/외부사용자 IP로 위장 후 서버에 접근

둘째, 내부 사용자는 비밀번호 해킹 프로그램 또는 사용인가자의 정보로 시스템 접근

- 취약점 분석 또는 Scan공격 등으로 해당 서버의 취약점을 분석한 뒤 접근

셋째, 서버접속 후 계정권한 변경 및 시스템 권한의 유령 사용자 등록

- 트로이 목마 삽입후 지속적인 공격 등으로 시스템을 공격

넷째, 정보획득 후 접속흔적 삭제

다섯째, 현 정부기관의 네트워크 및 정보보호 시스템은 논리적으로 인터넷과 분리되어 있는 관계로 Worm, DDos와 같은 신종 공격에 대한 대비책이 전무하거나 미비한 실정이다.[7-10]

3.3 역할기반 보안정책을 이용한 정부기관 환경 정보보호시스템 모델

3.1 정부기관 환경의 특징과 3.2 현 정부기관의 전산망특징에서의 문제점을 극복 및 충족시키기 위하여 본 논문에서는 정보보호시스템의 보안정책을 IPS와 역할기반 보안정책으로 하는 것을 제안한다. 역할기반 보안정책은 각 역할에 대하여 자원접근 권한을 허용하기 때문에 동적인 보안정책 변경이 가능할 뿐 아니라 내부 사용자에 대한 자원 접근권한 통제가 가능하므로, 정부기관의 정보보호 시스템이 가져야 하는 특징들을 충족시킬 수 있으며, IPS의 설치로 Worm, DDos와 같은 신종 공격방법에 대한 내구성을 확보할 수 있다.

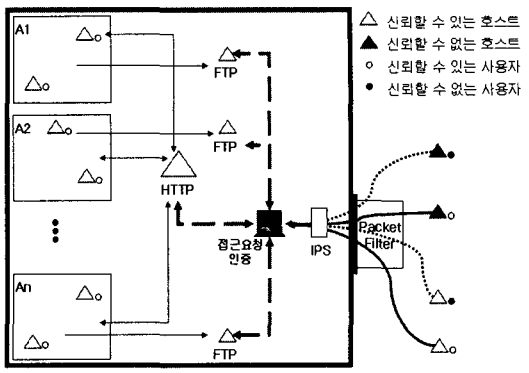


그림 4. 본 연구에서 제안하는 정부기관 정보보호 시스템

그림 4는 N개의 업무가 진행되는 업무 및 상황을 역할기반 보안정책을 적용하여 나타낸 것이다.

업무 A1은 내부담당자들과 공동작업을 하고 An은 외부기관과 공동작업 및 민원지원을 한다고 하자. 역할기반 보안정책을 적용하기 위하여

1) 업무단위별로 도메인을 구성(A1, A2 … An)하고,
2) 각 업무담당자별로 역할을 할당한다.
3) 접근 요청인증서버에 담당자별 권한정보를 입력한다.

이러한 경우 보안담당자는 업무단위별 업무담당자의 역할을 할당하여 담당자별 자원접근 권한을 할당한다. 제안 시스템의 [접근 요청인증]서버는 이러한 담당자별 자원접근 권한을 지정/관리하는 서버로서 모든 업무담당자들은 이 접근요청인증 서버를 거쳐서만 타 자원에 접근이 가능하다. 따라서 업무담당자들은 자신의 업무를 처리하기 위하여 필요한 자원에 대한 권한을 가질 수 있으며, 자신이 속하지 않는 업무는 할당된 자원이 없으므로 자원 접근이 불가능하다. 또한, 외부의 신뢰할 수 있는 사용자는 정보보호시스템의 외부에 있지만 업무 An에 대하여 인가된 자원을 가지고

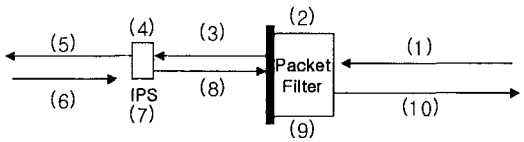


그림 5. Packet Filter와 IPS역할

있으므로, 인증과정(PKI)을 거친 후, An에 대한 접근이 가능하다.

제안하는 망에 대하여 외부부분과 내부부분 2가지로 분류하여 정보이동과 장비별 기능에 대하여 설명하겠다.

(외부는 Pacet Filter와 IPS로, 내부는 각 Server와 접근요청 인증서버로 구분하겠다.)

먼저 제안하는 망에서의 외부 정보흐름은 그림 5처럼 된다.

가. ①~⑤는 외부 사용자가 내부로 접근할 시의 경로도이다.

- ②는 외부 사용자에 대한 기본적인 Packet Filter를 하는 곳으로 IP등을 통제하여 접근을 제한하는 것이다.
- ④는 ②의 Filter를 ③의 정보를 다시 한번 유해성을 검사하는 단계로서, 이 단계에서는 Worm, DDos등의 신종 공격에 대한 Filter 작업을 한다. 여기서 ④의 역할은 매우 중요하다. ④는 Worm, DDos와 같은 네트워크상의 트래픽을 증가시키는 공격에 대한 차단작업 및 기타 유해 트래픽에 대한 차단하는 임무를 가지게 되는데 이는 네트워크의 자원과 안전성을 유지하기 위하여 매우 비중있는 역할을 하게 된다. 또한 ④의 단계는 기존의 Firewall이나 IDS보다 더욱 적극적으로 능동적으로 작동이 되므로, 관리자는 상시 모니터링 하는 시간적/공간적인 제약을 벗어날 수 있다.
- ④의 단계를 지난 ⑤는 접근요청 인증서버에서 해당 Server에 대한 접근을 요청하게 된다.

나. ⑥~⑩은 내부 사용자가 외부로 접근할 시의 경로이다.

- ⑥은 접근요청인증 서버로부터 내부에서 외부로 접근을 인증받은 정보들이다.
- 이 정보는 ⑦의 IPS시스템에서 Worm, DDos와 같은 공격등을 제거한다. 여기서 ⑦의 역할은 ④와 같이 Worm과 같은 공격들로부터 네트워크의 안정성 및 자원을 확보하는데 있다. 이미 인증을 거친 정보가 ⑦을 거치는 이유는 내부 사용자에 의한 Worm, DDos등과 공격으로 인한 네트워크를 보호하기 위함이다. ⑦에서 Filter가 된 ⑧은 다시 한번 ⑨에서 Filter를 거치게 된다.
- ⑨의 역할은 인증되었더라도 특정포트 및 IP에 대한 차단 역할을 하게 된다.

내부 정보흐름에서 서버에 대한 접근요청인증은 그림 6의 과정을 거치게 된다.

1) A1~An의 Server가 X라는 사용자의 접근요청 또는 기타처리에 관한 요청을 받았을 시
2) A1~An의 Server는 접근요청인증서버에 자신이 가진 권한정보를 암호화하여 전송(전송정보는 ID/PASS정보)
3) 접근요청인증서버는 자신이 가진 권한정보에서 해당정보를 찾아 승인 및 권한정보를 요청서버에 암호화하여 통보한다.(전송정보는 인증정보, 사용권한 정보)
4) 이 통보를 받은 A1~An Server는 자신이 가지고 있는 권한 정보화 비교한다.(접근요청인증서버로부터 받은 정보를 사용자가 접근할 수 없는 X라는 위치에 임시로 암호화하여 저장한 후 동일한 내용에 대하여 추후 요

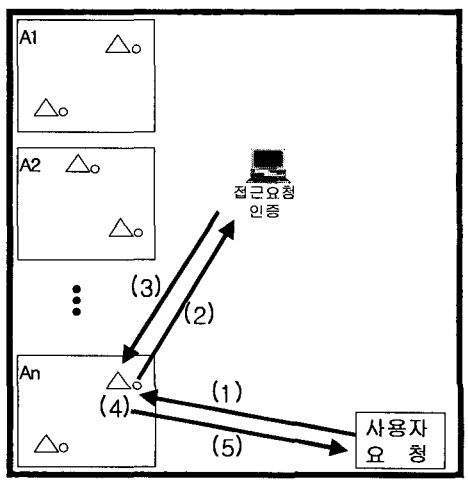


그림 6. 서버에 대한 접근요청 인증과정

청부터는 접근요청 인증 서버가 아닌 임시저장 정보로부터 권한을 정보를 가져온다. 단, 권한정보는 사용자 Logout후 또는 사용자가 일정시간이상 경과시 자동 삭제된다.)

5) 해당 정보에 대한 통보를 사용자에게 한다.

내부 정보흐름에서 사용자가 외부 시스템에 접근을 요청할 시에는 그림 7과 같은 과정을 거치게 된다.

이 경우는 위의 서버에서 요청인증 서버로 인증을 받는 경우와 차이가 있다.

여기서 접근요청 인증서버는 각 내부 사용자 PC별 권한을 가지고 있어야 한다. 즉, 접근요청 인증서버는 사용자의 요청에 대하여 자신이 가진 정보와 비교하여 외부 접근을 통제 하는 것이다.

(1)은 사용자가 생각하는 외부로 접근하는 경로이다.

(1-1)은 실질적으로 사용자가 외부로 접근하는 경로를 나타낸 것이다.

(1-1)의 정보는 접근요청 인증서버에서 가지고 있는 정보와 비교하여 허용시는 (1-3)으로, 불요시는 (1-2)로 정보를 전송한다. (1-2)의 경우에는 접근 Error 메시지를 출력하거나 권한제한 메시지를 출력해준다.

(1-3)을 통과한 정보는 IPS와 Packet Filter에서 추가적인 Filter를 걸치게 된다.

위의 2가지 외부 및 내부 정보흐름에서 중요한 점은 주요 접근정보(login, ftp등)에 대하여 반드시 접근요청 인증서버를 거쳐야 한다는 것이다.

또한, Server-접근요청 인증서버간에는 지정된 포트로만 전송을 해야 하며, 해당 포트는 주고받는 모든 정보를 암호화 및 복호화를 하여야 한다. 이는 불법적으로 정보 획득 및 변조에 대한 보호 차원이다. 이와 같은 방법으로 자료 처리시 에는 동시 요청이 증가 시에는 암호/복호화 및 접근요청/인증 처리과정에서 발생하는 트래픽으로 인하여 네트워크망의 속도 저하가 발생될 수 있다.

3.4 접근요청 인증서버 구조

3.2, 3.3에서 제기한 바와 같이 역할인증 시스템은 접근제어 정책의 설정을 다수의 서버 및 사용자에 대하여 시행하고 있다. 이때 추가/설정하고자 하는 정책의 적용 대상은 망에 연결된 모든 근원지와 목적지의 집합이 되며, 시스템의 구조는 그림 8과 같이 입력부와 저장부 그리고 입력/출력시 암호화 및 복호화 부분으로 구성되어 있다.

먼저 인증서버로 부터의 인증요청에 대한 처리과정은 1)에서 인증요청정보가 들어오면 해당내용을 복호화후 조회를 하게 된다.

3)조회명령은 DB에서 해당정보를 찾은뒤 다시 암호화를 하여 전송하게 된다. 요청서버는 암호화된 (6)의 정보를 받아 인증여부를 처리하게 된다.

일반 사용자가 외부망으로 나가고자 할시에는 1)에서 사용자IP, 접속하고자 하는 외부 IP, 접속방식등의 정보가 들어오면 복호화 단계를 거치지 않고 바로 검색모듈에서 권한을 체크한다. 만약 권한이 없는 곳이라면 패킷의 이동을 막은 후 사용자에게 에러 메시지를 전송한다.

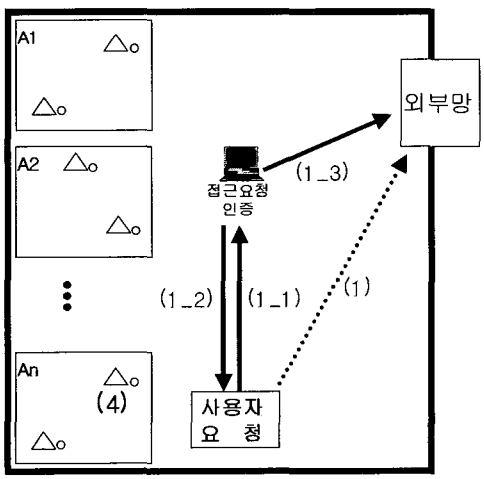


그림 7. 사용자 외부접근 요청과정

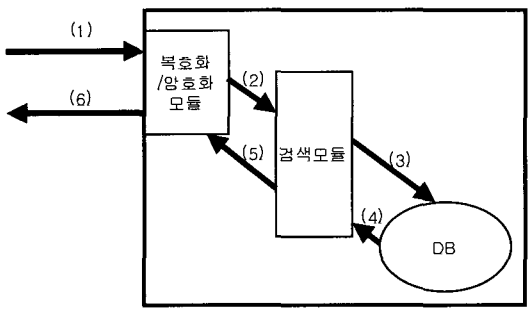


그림 8. 인증서버 구조

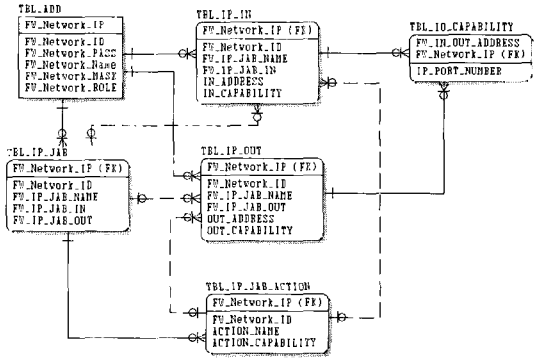


그림 9. 인증서버 DB구조

여기서 역할인증 시스템은 그림 9, 표 6과 같은 테이블 구조 및 역할을 가지게 된다.

표 6. 각 테이블별 역할

	테 이 블 명	역 할
1	TBL_ADD	접속 PC/SERVER에 대한 인증
2	TBL_IP_JAB	접속 PC/SERVER접근 사용자에 대한 인증
3	TBL_IP_IN	내부망으로 접근하는 사용자/PC등에 대한 권한
4	TBL_IP_OUT	외부망으로 나가는 사용자/PC등에 대한 권한
5	TBL_IO_CAPABILITY	내/외부 사용자별 PORT 접근권한
6	TBL_IP_JAB_ACTION	접근사용자별 명령권한

① 서버에서 인증서버로 정보를 요청시 : 서버 인증요청시 받는 정보는 서버IP(FW_Network_IP)/인증ID(FW_Network_ID)/인증PASS(FW_Network_PASS)/서버요청사용자ID(FW_IP_JAB_NAME)/사용명령(ACTION_NAME)이 된다.

이 경우 TBL_ADD에서 해당 서버에 대한 접속권한에 대하여 확인하고, 서버의 사용자 이름이 등록되어 있는지 확인을 하게 된다. 그 후 명령어에 대한 권한을 점검하게 되는 것이다. 명령어가 측정 PORT를 사용하는 경우에는 TBL_IO_CAPABILITY에서 해당 포트에 대한 권한 확인이 가능하다. 서버에서 TELNET을 할 경우 서버에 요청한 사용자에 대한 IN/OUT Port에 대한 권한을 점검하면 권한에 대하여 확인이 가능하다.

② 내부(개인)사용자가 외부로 접근 요청시 : 일반사용자가 서버를 거치지 않고 외부로 접속할 시 인증 서버는 사용자 IP(FW_Network_IP)/접속요청 IP(OUT_ADDRESS)/요청 PORT(IP_PORT_NUMBER) 정보를 받으며, 접속 후 특정 명령을 구동시에는 ①과 같은 절차를 거치게 된다.

③ 외부사용자가 내부로 접근요청 시 : 외부에서 내부로 접근요청 시에는 외부접근 IP주소(FW_Network_IP)/접근요청IP(IN_ADDRESS)/접근PORT(IP_PORT_NUMBER) 정보를 받아 권한을 점검하게 되며, 접속 후 특정 명령을 구동시에는 ①과 같은 절차를 거치게 된다.

Ⅳ. 현 정부기관 시스템과 제안 시스템 비교분석

본 연구에서 제안한 IPS와 역할기반보안정책을 이용한 정보보호시스템과 현 정부기관 정보보호시스템의 장단점을 상호 비교하면 표 7과 같다.

따라서, 본 논문에서 제안한 바와 같이 정보보호 시스템에 역할기반 보안정책을 적용하면 3.1과 3.2에서 제시된 환경정 특징과 문제점중 다음과 같은 사항을 만족시킬 수 있다.

가. IPS의 기능으로 Worm과 같은 외부에서의 침입행위에 대한 최소한의 방어 및 격퇴가 가능하다.

나. 정보보호 시스템 내부의 업무담당자도 적절한 권한을 가진 경우에만 정보보호 시스템 내부 자원에 접근이 가능하다. 즉, 역할기반 보안정책으로 인하여 보안정책 관리자가 역할을 할당하는 것에 따라 업무담당자의 자료접근을 통제할 수 있다. 따라서 정보보호 시스템 내부 사용자에 대한 보안정책의 문제점을 해결할 수 있다.

다. 정보보호 내부의 모든 "응답" 패킷은 "접근요청 인증 서버"에서 처리하여 인가된 권한을 가진 "응답"패킷만이 정보보호 내부의 자료에

표 7. 현 정보보호 시스템 및 제안정보보호시스템 비교

	현 정부기관 정보보호시스템	제안 정보보호 시스템
문제점	1. 내부사용자에 대한 해킹에 대하여 취약하다 2. 내부에서 Worm, DDos등과 같은 공격이 발생시에는 신속한 조치가 제한된다. 3. 내부 네트워크망 접근 가능시 모든 네트워크에 대한 접근이 가능하다. 4. 사용자 권한 해킹시 제한자료에 대한 접근이 가능하다. 6. 시스템 관리자의 지속적인 모니터링이 필요하다	1. 인증과정에서 네트워크 트래픽이 발생한다.
장점	1. 네트워크가 정상인 경우에는 트래픽이 적게 발생한다.	1. 내·외부 침입자에 대한 방어력이 좋다. 2. Worm, DDos와 같은 신종 공격에 대하여 신속한 조치가 가능하다 3. 내·외부 네트워크에 대한 접근 통제가 가능하다 4. 사용자 권한에 대한 신뢰도를 증가 시킬 수 있다. 5. 지속적인 모니터링이 불필요하다.

대하여 접근이 가능하다. 즉, 역할기반 보안정책을 적용한 정보보호 시스템은 외부에서 "응답" 패킷이 정보보호 시스템 내부로 들어와도 "접근용청 인증 서버"의 검증을 받지 않는 한 자료 접근을 통제할 수 있다. 따라서 정보보호시스템 외부에서 "응답" 형식을 가지는 패킷은 정보보호시스템 내부로 접근을 제한 할 수 있으므로 외부 패킷에 대한 보안상의 문제점을 극복할 수 있다.

라. 정보보호 외부 시스템의 사용자는 자신의 역할에 해당하는 정보보호 시스템 내부 자료에 접근이 가능하다. 즉 정보보호시스템 외부에 있는 사용자가 내부 자원에 접근하기 위하여 패킷 및 인증을 걸쳐 접근 요청을 하면 "접근요청 인증 서버"는 해당 사용자에 대한 권한을 확인 후 작업 자원에 대한 접근을 결정한다. 이러한 인증과정은 사용자 계정 및 비밀번호를 이용할 수 도 있으며, PKI와 같은 암호화 기법 등을 이용하여 사용할 수 도 있다. 또한, 역할기반 보안정책을 적용한 경우에는 외부에서 접근이 가능한 사용자를 별도로 묶어서 비인가 사용자에 대한 접근을 제한할 수 있어, 정보보호 외부 시스템에서도 인가된 사용권한을 가진 사용자는 정보보호 내부 시스템을 사용할 수 있는 정보공유/공개에 대한 문제점을 극복할 수 있다.

마. 내부사용자가 불법적으로 자료를 외부로 전송(같은 망을 사용한다는 전제하)하는 문제점을 극복할 수 있다. 즉, "접근요청 인증 서버"에서 자료의 접근 및 전송에 관한 모든 "응답" 및 "요청' 패킷을 관리하므로 내부사용자의 불법적인 자료 전송을 사전에 차단할 수 있다.

바. 외부 불법 접근자가 내부인증 사용자로 IP 변환하기전 발견/차단이 가능하다.

사. 불법접속을 하더라도 인증서버와 접근서버 두곳에 접속정보가 저장되기 때문에 접속흔적을 삭제하기가 불가능하다.

본 논문에서 제안한 정보보호시스템은 기존의 정보보호시스템에서 가지는 문제점 중 많은 부분을 처리할 수 있는 장점을 가지고 있다. 그러나 불법사용자가 외부 인가IP로 위장시에는 사용자 확인이 불가능하다는 문제점은 해결이 되지 않았으며, 내부 처리에 따른 트래픽량의 증가로 인하여 대규모 처리가 요구되는 업무에 적용시에는 적용이 제한되는 문제점이 예상되며, 접속로그의 이중저장으로 인한 저장공간의 소요가 증가된다. 따라서 본 논문에서 제시한 시스템은 신속한 처리를 요하는 시스템이 아닌 안정적이고 처리시간의 제약을 받지 않는 시스템이나 사용자가 접근이 제한되는 시스템에 부분적으로 적용하는 방안이 적합하다고 판단된다.

V. 결론 및 향후 연구

본 논문에서는 기존 네트워크 정보보호체계를 기반으로 하여, IPS와 역할기반보안 정책을 이용하여 좀더 효율적인 정부전산의 정보보호체계 방식을 제시하였다. 본 논문에서 제시한 정보보호체계의 장점은 기존에 설치되어 있는 정보보호체계와 병행하여 사용이 가능하다는 것이다. 즉, 기존의 정보보호 또는 IDS등과 같은 정보보호체계가 설치되어 있더라도 운영상 제한이 없으며, 오히려 기존 정보보호시스템이 정보보호체계의 기능을 향상시켜주는 역할을 하게 된다.

그러나, 본 논문에서 제시된 IPS와 역할기반 보안정책을 이용한 정보보호시스템은 기존의 정보보호 시스템에서보다 더 많은 네트워크 트래픽 발생 및 자원을 요구하게 된다. 따라서 본 논문에서 제시한 인증관련 트래픽으로 인한 응답지연에 대한 분석과 연구가 필요하다.

참 고 문 헌

[1] Nicholas Yialeis, Emil Lupu, Morris Sloman, "Role-based security for distributed object system," in Proceedings of the 5th Workshops on Enabling Technologies, Infrastructure for Collaborative Enterprises(WET ICE '96)(96TB100058). Los Alamitos, CA, USA : IEEE comput. Soc Press, 1996. p. 80-5 of xii+ 353 pp.

[2] PLUS(포항공대 유닉스 보안 연구회), Security PLUS for UNIX, 영진.com, 2001

[3] 박재근, "전사적 국방정보보호관리체계 구축방안", "제5차 통신전자정보화 학술대회", pp. 77-82, 2001.9]

[4] 한국정보보호센터, 정보보호개론, 교우사, 2000

[5] "차세대 보안솔루션 IPS공개 평가 세미나 자료", 정보보호21c, 2004년 3월 10일

[6] "기업 정보보호 실천 가이드 2004 정보보호 솔루션·서비스 도입사례 BEST 63", 정보보호21c

[7] 한국전산원, "2001 국가정보화백서", 한국전산원, 2001

[8] 한국전산원, "2002 국가정보화백서", 한국전산원, 2002

[9] 한국전산원, "2002년 공공부문 정보자원 현황분석", 한국전산원, 2002

[10] 한국전산원, "공공부문 정보통신망 구축 표준모델 연구", 한국전산원, 2003

[11] 홍승욱, "IDS(침입탐지시스템) 토요 세미나 자료", 2002.3

[12] 안현구, "네트워크 타임즈 /55호 240-245페이지", 1998.3

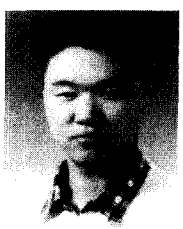
[13] 김우일, "방화벽 시스템에 대한 고찰", 1999.10

[14] 한국 정보보호 진흥원(HTTP://www.kisa.or.kr)

[15] 인터넷 사이트, http://www.sisait.co.kr/column/200112/solution/solution_entercept.htm

[16] 기타 인터넷 보안관련 사이트

〈著者紹介〉



안 정 철 (Joung-Choul Ahn) 학생회원

1998년 2월 : 밀양산업대학교 컴퓨터공학과 졸업(공학사)
2004년 2월 : 세종대학교 정보보호학과졸업 (공학석사)
1998년 3월~2003.6 : 해병대 통신/전산장교
2003년 9월 ~ 현재 : 한국 국방연구원 연구원 재직중
〈관심분야〉 정보보호정책, 정보보안, 정보보호시스템, 유비쿼터스