역할기반 보안정책을 이용한 연구 환경 방화벽 시스템 설계

신훈철*, 이금석
동국대학교 컴퓨터공학과

A Design of Research Environment Firewall System using Role-Based Security Policy

Hoonchul Shin*, Keumsuk Lee
Dept of Computer Engineering, Dongguk University

요 약

지금까지 방화벽 시스템에 대한 연구는 정보에 대한 접근을 최대한으로 제한하는 "기본 거부(Default Deny)" 정책을 중심으로 연구되어 왔다. 그러나 대학 및 연구소와 같은 환경(이하 연구 환경)에서는 많은 연구 과제들이 동시에 수행되고, 또한 이러한 정보들이 외부와 공동으로 진행되는 경우에 정보를 공유할 뿐만 아니라 연구 결과를 외부에 공개할 필요성이 있다. 따라서 연구 환경에 대한 보안정책은 기존의 기본 거부 정책보다는 정보에 대한 "개방성"이 요구된다.

따라서 본 연구에서는 연구 환경에서, 정보의 공유 및 공개를 위한 "개방성"을 충족시키기 위하여 역할기반 보안정책(Role-Based Security Policy)을 이용한 방화벽 시스템을 제안한다. 역할기반 보안정책을 적용함으로서 방화벽 시스템 내부 사용자에 대한 보안정책 적용이 가능할 뿐만 아니라, 방화벽 시스템 운용시에도 사용자의 역할 할당 및 변경 등의 보안정책 변경이 가능하다

1. 서론

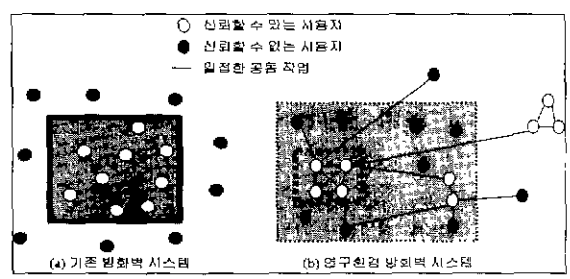
현재까지 방화벽 시스템에 대한 많은 연구가 진행되었다. 기존에 연구된 방화벽 시스템은 자원의 사용을 최대한으로 억제하는 이른바 "기본 거부" 정책을 중심으로 연구되었다. 즉, 방화벽 시스템에 미리 등록된 인가(Authorization)된 권한을 가진 사용자는 자원에 대한 접근이 허가되는 반면, 등록되지 않은 사용자에 대해서는 자원에 대한 접근을 엄격히 제한한다. 이러한 보안정책을 적용하기 때문에 방화벽 시스템은 TCSEC(Trusted Computer System Evaluation Criteria)의 B2 보안 등급에 해당한다.

그러나 연구 환경에서의 방화벽 시스템은 기존의 방화벽 시스템에서 사용한 "기본 거부" 정책과는 달리 정보의 공유 및 공개를 위한 "개방성"을 요구한다[1]. 즉, 연구 환경은 그 자체적인 특성상, 연구 환경 외부와 공동으로 연구 과제를 수행하며, 이러한 결과들을 외부와 공유 또는 공개할 필요성이 있다.

(그림 1)은 기존 방화벽 시스템과 연구 환경 방화벽 시스템에서 보안정책 적용 범위를 비교한 것으로서, 기존 방화벽 시스템은 (a)와 같이 보안정책 적용 범위를 명확히 구분할 수 있지만, 연구 환경 방화벽 시스템은 (b)와 같이 그 경계를 명확히 구분할 수 없다[1].

따라서 본 논문에서는 역할기반 보안정책을 이용하여 연구 환경에서 요구되는 "공개성"을 충족시키고, 또한 보다 추상화된 방법으로 정책을 표현할 수 있는 방법을 제안하였다.

본 논문에서는 2장에서 관련 연구를 살펴보고, 3장에서 연구 환경의 특성을 살펴보고, 그 특징들을 충족시킬 수 있도록 역할기반 보안정책을 이용한 방화벽 시스템 모델을 제안한다 4장에서는 결론 및 향후 연구에 대하여 논하였다.



(그림 1) 방화벽 시스템의 포용범위

2. 관련연구

2.1. 연구 환경 방화벽 시스템

스탠포드 대학에서는 (그림 2)와 같이 연구 환경에서의 방화벽 시스템을 제안하였다. 그러나 이 방화벽 시스템은 내부 네트워크 사용자에 대해서는 모두 신뢰할 수 있다는 가정 하에 설계된 시스템으로서, 방화벽 시스템 내부 사용자에 대해 보안정책을 적용하기에는 미흡한 면이 있다. 또한 현재 가장 널리 사용되는 3-단계 프로토콜인 TCP를 위주로 설계하였기 때문에, TCP 프로토콜이 가지는 보안상의 문제점[2]을 내재하고 있다

이 방화벽 시스템은 다음과 같은 목표를 가지고 설계되었다[1]

① 방화벽 시스템 내부에서는 임의의 외부 시스템을 사용할 수 있다 (Request-Reply Policy)

② 방화벽 시스템 외부에서 접근할 수 있는 공개된 시스템이 필요하다.(Exposing a Secure Public Image)

③ 방화벽 외부 시스템에서도 인가된 사용권한을 가진 사용자는 방화벽 내부 시스템을 사용할 수 있다.(Secure Non-Local Access)

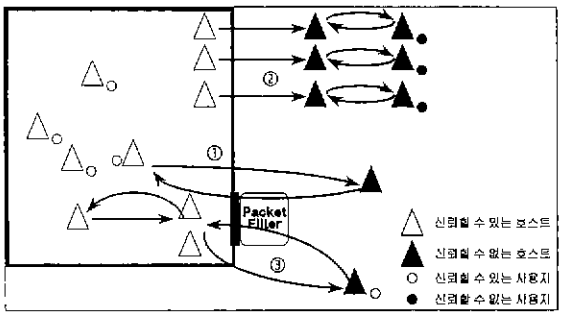
그러나 이 방화벽 시스템은 현재 가장 널리 사용되는 TCP 프로토콜과 같은 방식인 "요청-응답(Request-Reply) 정책"을 사용하기 때문에 TCP 프로토콜과 같은 연결지향형 3-단계 프로토콜에는 적합하지만, IP 프로토콜과 같은 비접속형 프로토콜에는 부적합할 뿐만 아니라, 다음과 같은 문제점을 가지고 있다[1].

① 방화벽 내부의 정보는 방화벽 시스템 외부로 쉽게 유출될 수 있다.

② 외부에서 "응답" 형식을 가진 패킷은 방화벽 시스템 내부로 들어올 수 있다.

③ 외부에서 한번 인증된 시스템 및 사용자는 방화벽 시스템 내부 정보를 사용할 수 있다.

따라서 네트워크 상에서 보안을 유지하기 위해서는 근본적으로 현재 널리 사용되는 TCP/IP 프로토콜 자체에 대한 보완이 필요하다[1][2]



(그림 2) 스탠포드에서 제안한 연구 환경 방화벽 시스템

2.2. 역할기반 보안정책

분산 시스템 환경의 사용이 증가됨에 따라 관리해야 할 자원과 사용자의 수가 매우 커졌다. 따라서, 분산 시스템의 보안 측면에서 기존에 사용하던 패킷 필터링 규칙 위주의 접근 제어 목록(Access Control List)만으로는 정책의 충돌(Conflict) 및 보안정책 관리자의 오류 등을 분석하기 어려울 뿐만 아니라 정책 구현에 대한 검증이 어렵다 따라서 분산된 자원의 관리와 보안을 용이하게 하고 대규모 시스템의 관리 책임을 분산시키기 위하여, 공통된 정책을 적용할 대상을 도메인(Domain) 단위로 구성하는 역할기반 보안정책 모델[3]에 대한 연구가 진행되었다. 이 모델에서는 자원 접근을 요청하는 주체(Subject)와 그 요청을 받아들이는 객체(Object)로 구분하고, 주체와 객체 사이에는 주체가 객체에 행할 수 있는 역할(Role)로써 관계가 맺어진다. 주체나 객체는 도메인 단위로 구성될 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 할 것을 의미한다 주체와 객체 사이의 관계를 역할로 표현함으로써, 역할에 적용되는 정책을 재구성할 필요 없이 개인에게 역할을 할당하거나 회수하는 등의 방법으로 정책의 변경이 가능하다[3].

3. 역할기반 보안정책을 이용한 연구 환경 방화벽 시스템

본 논문에서는 연구 환경의 특징들을 살펴보고, 연구 환경에서 방화벽 시스템을 사용할 경우, 이러한 특징들을 모두 반영하기 위하여 역할기반 보안정책 적용을 제안한다. 또한 보안정책 결정시 발생할 수 있는 보안정책 충돌에 대한 문제를 고려하였다.

3.1. 연구 환경의 특징

연구 환경 방화벽 시스템은 "개방성"의 특징을 가져야 하지만, 스탠포드 대학에서 연구한 방화벽 시스템은 너무나 많은 "개방성"으로 인하여 2.1 절에서 언급한 문제점들이 발생한다. 그리고, 방화벽 시스템 내부의 사용자와 시스템은 모두 신뢰할 수 있다는 전제 조건 때문에 실제 방화벽 시스템 환경 구축에 적합하지 못하다.

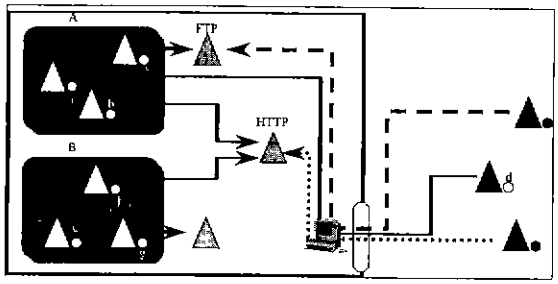
본 연구에서는 [1]에서와 같이 너무나 많은 "개방성"으로 인한 문제점을 개선하고, 연구 환경에 적합한 보안정책을 반영할 수 있는 방화벽 시스템을 위하여 다음과 같이 연구 환경의 특징을 요약하였다.

첫째, 연구 환경에서는 동시에 여러 개의 연구과제가 진행 가능하고, 연구과제 간의 관계 또는 연구과제와 연구원들 간의 관계가 매우 복잡해 질 수 있다. 하나의 연구과제를 진행하기 위해서는 연구원들 간에 주어지는 역할에 따라서 자원에 대한 접근 권한이 다를 수 있다 예를 들면, 연구과제 총 책임자는 해당 연구과제에 대한 모든 자원에 대해서 접근 가능해야 하고, 각 연구원들은 자신이 맡은 부분에 대한 자원 접근 권한을 가져야 한다. 둘째, 방화벽 시스템 내의 사용자를 모두 신뢰할 수 있는 것은 아니다. 즉, 각 연구원들은 자신이 속한 연구과제에 대한 자원 접근 권한만을 가져야 하며, 자신이 속하지 않은 다른 연구과제의 자원에 대한 접근 권한은 허가되어서는 안 된다 셋째, 방화벽 시스템에 적용되는 보안정책은 시스템 운용 중에 동적으로 변경될 수 있어야 한다 즉, 하나의 연구 과제가 끝나거나 또는 구성원이 변경되는 경우 이를 방화벽 시스템 운용 중에 보안정책에 반영할 수 있어야 한다.

3.2. 역할기반 보안정책을 이용한 연구 환경 방화벽 시스템 모델

역할기반 보안정책은 각 역할에 대하여 자원 접근 권한을 할당하기 때문에 동적인 정책 변경이 가능할 뿐만 아니라, 방화벽 시스템 내부의 사용자에 대해서도 자원 접근 권한을 설정 가능하다. 따라서 연구 환경에서 가져야 할 특징들을 모두 충족시킬 수 있다.

(그림 3)은 연구 환경에서 두 개의 연구과제가 진행되는 상황을 역할기반 보안정책을 적용하여 나타낸 것이다. 연구과제 A는 방화벽 시스템 외부와 공동작업을 진행하고, 연구과제 B는 방화벽 시스템 내부의 연구원들만으로 작업을 진행한다. 역할기반 보안정책을 적용하기 위하여 연구작업 단위로 도메인을 구성하고(A, B), 각 연구과제별로 연구원의 역할(a, b, c, d, e, f, g)을 할당한다 이러한 경우 보안정책 관리자는 연구과제를 수행하는 연구원들에게 자원 접근 권한을 할당하기 위해서 각 연구과제별 연구원의 역할을 할당한다 따라서, 연구원들은 자신이 속한 연구과제를 수행하기 위해 필요한 자원들에 대한 접근 권한을 가질 수 있다. 그러나 자신이 속하지 않은 연구과제에 대해서는 할당된 역할이 없으므로, 자원 접근이 불가능하다 또한 d는 방화벽 시스템 외부에 있지만 연구과제 A에 대해 인가된 역할을 가지게 되므로, 인증 과정을 거친 후, A의 자원에 대한 접근이 가능하다.



(그림 3) 본 연구에서 제안한 연구 환경 방화벽 시스템

따라서 본 논문에서 제안한 바와 같이 방화벽 시스템에 역할기반 보안정책을 적용하면 다음과 같은 사항을 만족시킬 수 있다.

① 방화벽 시스템 내부의 사용자도 적절한 권한을 가진 경우에만 방화벽 시스템 내부 자원에 접근할 수 있다. 즉, 역할기반 보안정책을 적용하였기 때문에 보안정책 관리자가 역할을 할당하는 데 따라서 사용자 및 연구원들의 자원 접근 권한을 제한하거나 허가할 수 있다. 따라서 [1]에서 방화벽 시스템 내부 사용자에 대한 보안정책 적용의 문제점을 해결할 수 있다.

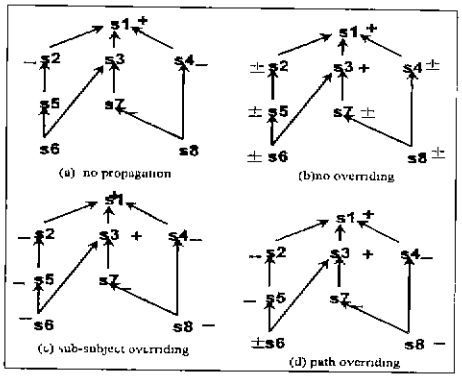
② 인가된 권한을 가진 "응답" 형식의 패킷만이 방화벽 시스템 내부의 자원에 접근할 수 있다. 역할기반 보안정책을 적용하면 방화벽 시스템 외부에서 "응답" 형식을 가진 패킷이 방화벽 시스템 내부로 들어온다 하더라도 그 패킷의 역할을 검사함으로써 자원 접근을 제한할 수 있다. 따라서 [1]에서 "응답" 형식을 가진 방화벽 시스템 외부 패킷이 발생시킬 수 있는 보안상의 문제를 해결할 수 있다

③ 방화벽 외부 시스템의 사용자는 자신의 역할에 해당하는 방화벽 시스템 내부 자원을 사용할 수 있다. 방화벽 시스템 외부에 있는 사용자가 내부 자원에 접근하기 위해서는 인증 과정을 거친 후, 그 사용자의 역할에 따라서 작업 접근 권한을 결정한다. 이러한 인증 과정은 사용자의 계정 및 패스워드를 이용함으로써 이루어 질 수 있고, 또한 안전한 정보 전송을 위하여 암호화 기법 등을 사용할 수 있다.

3.3. 충돌 해결(Conflict Resolution)

시스템 관리 측면에서 도메인 개념을 적용하는 경우에는 보다 자원을 효과적으로 사용하는 것이 궁극적인 목표이기 때문에, 관리 정책 기술 시에 고려할 사항이 매우 복잡하다. 즉, 사용자가 가진 권한 여부, 자원의 우선 순위, 책임과 권한의 상관관계, 권한 양도 시에 고려할 사항 등 여러 가지 경우를 고려해야 한다. 따라서 시스템 관리 정책을 설계할 경우에는 정책 충돌에 대하여 여러 가지로 고려해야 한다 그러나 시스템 보안 관리 측면에서는 어떠한 작업을 수행하기 위해서는 그에 해당하는 최소한의 권한만을 부여하는 "최소 권한(Least Privilege)"의 원칙[5]이 적용되어야 한다. 또한, 방화벽 시스템의 근본 목적은 "정보 보호"이므로, 보안정책에서 접근 허가와 접근 금지 권한이 충돌되는 경우 접근 금지 정책을 적용할 수 있다.

(그림 4)는 기술된 보안정책에서 자원 접근에 대한 충돌이 발생하는 경우를 보인 것이다. (a)가 처음 보안정책을 기술한 것이고, (b)는 각각의 권한이 모두 계승되는 경우인데, 여기서 ±가 충돌이 발생한 경우를 나타낸 것이다. (c)는 계승되는 권한 중에서 자신에게 가장 가까운 상위계층의 권한을 계승하는 경우이고, (d)는 +, -를 모두 계승받는 경우 이를 충돌로 간주하는 경우이다[3]. 본 연구에서는 (d)의 방법을 따르는 것을 기본으로 하고, 충돌이 발생한 경우 기본적으로 방화벽 시스템에서 사용되는 기본 거부 정책을 사용하여 자원 접근을 금지하도록 한다 즉, (그림 4)의 (d)에서 s6은 +, -권한을 모두 가지고 있지만, 실제적으로는 - 권한을 가지도록 하는 것이다.



(그림 4) 보안정책 충돌이 발생하는 경우

4. 결론 및 향후 연구

본 논문에서는 연구 환경에 대한 특성을 살펴보고, 연구 환경에서 정보의 공유 및 공개라는 특성을 충족시킬 수 있도록 방화벽 시스템의 보안정책으로서 역할기반 보안정책을 이용할 것을 제안하였다 또한 연구 환경에서 역할기반 보안정책을 이용한 방화벽 시스템 모델을 제시하였고, 보안정책 결정 시에 발생하는 정책 충돌에 대하여 방화벽 시스템에서 적용되는 "최소 권한"의 원칙을 적용할 것을 제안하였다.

기존 방화벽 시스템에서는 모든 패킷에 대하여 단순한 규칙들을 적용하지만, 역할기반 보안정책을 적용하기 위해서는 모든 패킷에 대하여 보다 많은 비교 연산이 행해져 패킷 필터링 속도가 떨어질 것이다. 따라서 향후 연구과제로서 역할기반 보안정책이 방화벽 시스템 운용에 적용되기 위해서는 보다 빠른 패킷 필터링에 대한 연구가 필요할 것이다.

또한 보안정책을 보다 효과적으로 반영하기 위한 근본적인 해결책으로서는 현재 가장 많이 사용되는 TCP/IP 프로토콜 자체에 대한 개선이 필요하며[1][5], 차세대 프로토콜에 대한 연구도 진행되어야 할 것이다.

참고문헌

[1] M.B. Greenwald, S.K. Singhal, J.R. Stone, D.R. Cheriton, "Designing an Academic Firewall," In OnTheInternet, Vol.2, No 3, May/June 1996, pp 24-33.

[2] Steve M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," ACM Computer Communications Review, Vol 19, No 2, March 1989

[3] Nicholas Yialeis, Emil Lupu, Morris Sloman, "Role-based security for distributed object systems," 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.

[4] S.Jojodia, P. Samarati, V.S. Subrahmanian, "A Logical Language for Expressing Authorizations," Proc IEEE Symp. On Security and Privacy, Oakland, Calif., May 1997, pages 31-42.

[5] D.B. Chapman, E.D.Zwicky, "Building Internet Firewall," O'Reilly & Associates, 1995.

[6] M.S Sloman, "Policy Driven management for Distributed Systems," Journal of Network and Systems Management, vol 2, no. 4, pp. 333-360, Dec. 1994.

[7] J.D. Moffett, "Policy Conflict Analysis in Distributed System Management," To be published in Journal of Organizational Computing Vol 4, No. 1 1994.