[9-21]

라우터의 안전한 네트워킹을 위한 정책 기반의 보안 관리

조 수 형, 은 성 경, 김 정 녀

한국전자통신연구원 정보보호연구단 보안운영체제연구팀

(shjo, skun, jnkim)@etri.re.kr

Policy-based Security Management for secure networking of Router

Su-Hyung Jo, Sung-Kyung Un, Jeong-Nyeo Kim

Secure Operating System Research Team, Information Security Research Division

Electronics and Telecommunications Research Institute (ETRI)

요 약

라우터는 네트워크의 데이터 패킷흐름을 제어하고 적합한 목적지에 도달하는 최적의 길을 결정한다. 라우터의 오류 또는 라우터에 대한 공격에 의한 피해는 전체 네트워크에 대한 피해가 될 수 있으므로, 라우터에 대한 접근 제어와 불법 네트워크 침입을 라우터에서 제어하는 보안 기술이 필요하다. 그리고, 보안 정책에 의한 관리 방법으로 보안 환경의 변화에 민첩하게 대처하고 통합된 관리 방법을 제시한다. 이 논문에서는 라우터나 게이트웨이 등의 네트워크 노드의 보안 문제를 해결하기 위해 패킷 필터링, 침입 분석 및 감사 추적, 인증 및 접근제어 기능의 보안 엔진을 제공하며, 이 보안 엔진을 보안 정책에 의한 관리를 제공하고자 한다. 패킷필터링 정책, 침입탐지 정책, 신뢰채널 정책, 접근제어 정책을 적용하여 네트워크 공격을 탐지하고, 통신채널에 기밀성과 무결성을 제공하며, 라우터의 접근을 통제하여 침입 탐지에서 대응까지 통합 보안을 제공하는 효과가 있다.

1. 서론

라우터는 네트워크의 구성 요소들을 연결하여 데이터 전송을 담당하는 장비로 최적경로를 설정하고 네트워크의 데이터 패킷흐름을 제어한다. 라우터는 내부와 외부를 연결하는 네트워크의 중요한 장비로 바이러스, 라우팅 프로토콜 공격, 서비스 거부 공격, 분산 서비스 거부 공격과 같은 네트워크 공격의 위협을 받고 있다. 이러한 네트워크 공격에 대응하기 위해 라우터에 대한 접근제어, 방화벽, 침입탐지 등의 보안 기술이 필요하다.

기존 네트워크의 보안 방식은 단일 기능의 개별적 보안 시스템 위주로 구현되어 보안 시스템간의 상호 연동이 어려우며 정보 보호 인프라의 구축이 복잡하고 어렵다. 정보 통신기술의 진화에 따라 새롭게 등장하는 보안 취약점에 따라 발생 가능한 여러 유형의 사이버 테러에 능동적으로 강력하게 대응할 수 있는 통합 보안 네트워킹이 요구되고 있다. 그리고, 보안 정책[1]이 없는 보안 관리 시스템은 보안 환경의 변화에 민첩하게 대처하지 못하고 통합된 관리 방법을 제시하지 못한다. 이러한 문제를 해결하기 위해 표준화된 보안 정책을 가지고 시스템을 분석하고 유지 보수할 수 있는 정책 기반의 보안 관리가 필요하다. 정책을 기반으로 한 통합된 보안 관리 기술은 라우터의 보안 문제를 관리하고 침입을 감지하며 이에 대응할 수 있다.

본 논문에서는 라우터나 게이트웨이 등의 네트워크 노드의 보안 문제를 해결하기 위해 보안 엔진의 구조와 정책 기반의 보안 관리 방법을 제시하였다. 네트워크 노드의 보안 엔진은 패킷 필터링, 침입 분석 및 감사 추적, 인증, 접근제어 및 정책관리 기능을 제공한다. 보안 정책을 기반으로 네트워크 노드를 관리하고, 정책의 교환과 협상을 위해 COPS [2]프로토콜을 사용한다.

본 논문의 구성은 다음과 같다. 2 장에서는 정책 기반 네트워크 관리에 대하여 알아보고 3 장에서는 보안 엔진의 구조와 정책 기반 보안 관리 시스템의 구조를 설계한다. 4 장에서는 설계를 바탕으로 구현