정책기반의 네트웍보안 관리 모델에 관한 연구

고종국*, 김정녀*

*한국전자통신연구원

Policy based Network Security Management Research

Jong-Gook Ko*, Jeong-Nyeo Kim*

*Korea Electronics and Telecommunications Research Institute

요 약

근래에 네트웍의 규모가 커지고 복잡해지고 있는 가운데 네트웍을 구성하는 각 노드들의 자체 보안 및 전체적인 관리에 관한 관심이 증가하고 각 보안 도구들의 통합적인 관리 또한 연구되어 지고 있다. 본 논문은 네트웍을 구성하는 노드들(라우터, 게이트웨이, 스위치 등)의 관리에 있어서 더 안전하고 효율적인 관리가 이루어지고 이들의 상호 작용을 통해 해커들의 침입을 방지하는 네트웍 보안 관리 시스템에 대한 연구 내용을 기술한다.

I. 서론

많은 인터넷 사용자의 증가와 기업의 복잡성 및 규모가 커지는 것으로 인해 네트웍의 규모가 점점 커지고 있는 가운데 네트웍의 보안 관리에 대한 관심과 필요성이 증가하고 있다. 또한, 해킹에 대한 여러 가지 대응 도구들이 하나로 통합되어 관리되는 ESM 과 같은 연구도 많이 진행되고 있다. 보안 관리에 있어서 정책 기반 관리[1]는 관리자가 수동적으로 모든 네트웍 구성 요소들을 관리하는데 필요한 많은 노력과 어려움을 줄이고자 하는데 목적이 있다. 정책기반 보안 관리 모델에는 다음과 같은 구성요소가 필요하다: policy console, policy management tool, policy repository, policy decision point(PDP), policy enforcement point(PEP). 먼저, Policy console 은 human netwok manager 와 policy management system 과의 인터페이스를 제어한다. 대부분의 정책 시스템 회사들은 GUI를 사용한다. policy console 은 policy 규칙들을 policy repository 로 저장하기 위한 형태로 바꾸기 위하여 policy management tool 과 함께 작업한다. policy management tool 의 많은 기능들은 policy console 상에서 진행되어 진다. 예를 들어 console에서 생성된 정책들을 translate 하고 console을 대신해서 policy repository 와 통신을 수행한다. 또한, policy management tool 은 정책에 있어서 변화에 대해서 policy decision point 에 알려주는 기능도 수행한다. policy repository 는 보안 관리 시스템을 위해 만들어지는 정책 규칙들을 저장하는 곳이다. 요즘은 LDAP 을 이용한 데이터 검색이 수행되어 지고 있다. policy decision point(PDP) 는 정의된 정책들을 PEP 가 이해할 수 있는 정책들로 바꾸는 기능을 수행하고 PEP 정책이 수행되도록 명령한다. 또한, 그러기 위해서 PDP 는 PEP 의 리스트를 유지하고 각 PEP 와 관계된 정책들을 DB 로 부터 가져올 수 있어야 한다. PEP 는 예를 들어 네트웍 트래픽을 처리하기 위해 PDP로부터 가져온 명령들을 수행, 적용한다. 네트웍의 통합적인 보안 관리를 위한 것 외에도 네트웍을 구성하는 각 노드들 자체의 보안도 중요하다. 예를 들어, 하나의 서브네트웍을 담당하고 있는 라우터가 외부의 침입으로부터 공격을 받았을 때, 그 라우터와 관계된 서브네트웍 또한 위협에 노출될 수 밖에 없다. 그러한 문제를 해결하기 위해서라도 네트웍을 구성하는 각 노드들의 자체적인 보안을 더 강화해야 한다. 본 논문에서는 네트웍을 구성하는 노드들의 관리에 있어서 더 안전하고 효율적인 관리가 이루어지고 이들의 상호작용을 통해 해커들의 침입을 방지하는 정책 기반의 네트웍 보안 관리 시스템에 대한 연구를 기술하고 네트웍 노드 자체의 보안을 위해 라우터와 같은 네트웍 노드의 보안 시스템 구조에 대해 기술한다.

2장에서는 정책 기반의 네트웍 노드들의 보안 관리 구성과 노드 자체의 보안을 위한 접근제어 기능 그리고 침입에 대한 대응 방법을 소개하고 3장에서는 결론 및 향후 과제에 대해 설명한다.

II. 본문

1. 네트웍보안관리 시스템 구성

전체적인 네트웍 보안관리 시스템의 구성을 위

해 라우터와 같은 네트워 노드에는 접근제어 기능과 침입 차단 기능, 정책 적용 기능, 그리고 침입탐지기능이 운영체제 레벨에서 제공되고 정책 결정 기능은 사용자 레벨에서 동작하며 소켓이나 COPS 와 같은 통신을 통해 원격 지에 있는 전체적인 보안 관리 기능을 담당하는 시스템과의 연동이 이루어진다. 접근제어 기능은 네트워 노드에 역할 기반의 접근제어[2][3]를 적용하여 비 인가된 사용자의 접근을 막고 슈퍼유저 권한 해킹에 대한 따른 피해를 최소화 하는 기능을 수행한다. 라우터의 필터링 규칙이나 라우터 테이블에 대한 해킹 피해로 인해 전체 네트워으로 피해가 확산되는 것을 막기 위해 각 네트워 노드들의 자체 보안을 우해 접근제어가 필요하다. 침입 차단 기능은 기본적인 패킷 필터링 기능으로 비 인가된 주소로부터 접근을 차단하는 기능을 수행한다. 침입 탐지 기능은 기존의 IDS(Intrusion Detection System)[4] 과 다르게 응용 수준에서 모니터링 하는 것이 아니라 운영체제 커널 내부에서 동작하도록 하여 패킷들을 하나도 빠트림 없이 검사하여 모니터 하는 기능이다. 정책 적용 기능은 정책 결정 기능으로부터 받은 정책을 적용하는 기능을 수행한다. 여기에서 적용되는 정책에는 접근제어와 관련하여 접근속성을 바꾸거나 패킷 필터링 규칙을 변경하거나 또는 침입 탐지 규칙을 변경하는 것들과 관련된 규칙들이다. 접근제어, 패킷 필터링, 그리고 침입 탐지 기능은 각각 침입이 발생된 정보를 정책 결정 기능을 통해 보안 관리 기능을 수행하는 원격 시스템에 보내고 그에 필요한 정책을 돌려 받는다. 마지막으로 원격에서 전체적으로 네트워 장치들과 통신하며 침입 정보들을 수집하고 그에 따른 정책을 보내는 보안 관리 기능이 있다. 그림 1은 네트워 보안 관리 시스템의 구성도를 나타낸다. 그림에서와 같이 기존의 커널에 시스템 자체 보안을 위한 접근제어 기능, 패킷 필터링기능, 침입 탐지 기능이 커널 레벨에서 동작하도록 되어 있다. 원격에 있는 보안 관리에서 정책을 보낼 때, 그 사이의 데이터 전송은 암호화가 되어져서 보내져야 한다. 암호화된 데이터의 전송은 보안 관리에서의 중요한 요소중 하나이다.

2. 접근제어를 통한 네트워 노드 자체 보안

네트워 보안 관리에 있어서 전체적인 보안 관리가 이루어져야 하기 위한 기본 요구사항으로 각 네트워 노드들의 보안성을 보장해야 한다. 기존의 라우터의 대표적인 해킹피해 유형은 SNMP의 취약성을 이용하여 루트권한 획득을 하고 난 후 라우팅 테이블이나 필터링 규칙들을 수정하는 유형이 있고 DOS 공격을 수행하여 라우터에 피해를 주는 유형들이 있다. 루트 권한 획득으로 인한 피해를 막기 위해 기존의 접근제어 이외에 라우터와 같은 네트워 노드 자체에 접근제어 기능을 추가하여 루트의 권한을 축소하는 방법을 사용할 수 있다. 본 시스템에서 사용되는 접근 제어는 역할 기반 접근제어이다. 역할기반 접근제어는 정보에 대한 사용자의 접근은 개별적인 신분이 아니라 조직 내에서 개인의 역할(직무)에 따라서 결정된다. 아래 그림 2 는 역할 기반 접근제어의 기본 개념이다. 기존의 user, group, other 들로 이루어진 신분 기반의 접근제어에서는 사용자와 권한이 직접 연결되어 있어서 관리에 어려움이 있지만 역할 기반 접근제어에서는 그 사이에 인터페이스 역할을 수행하여 접근제어 관리에 보다 편한 관리 기능을 제공할 수 있다. 본 시스템

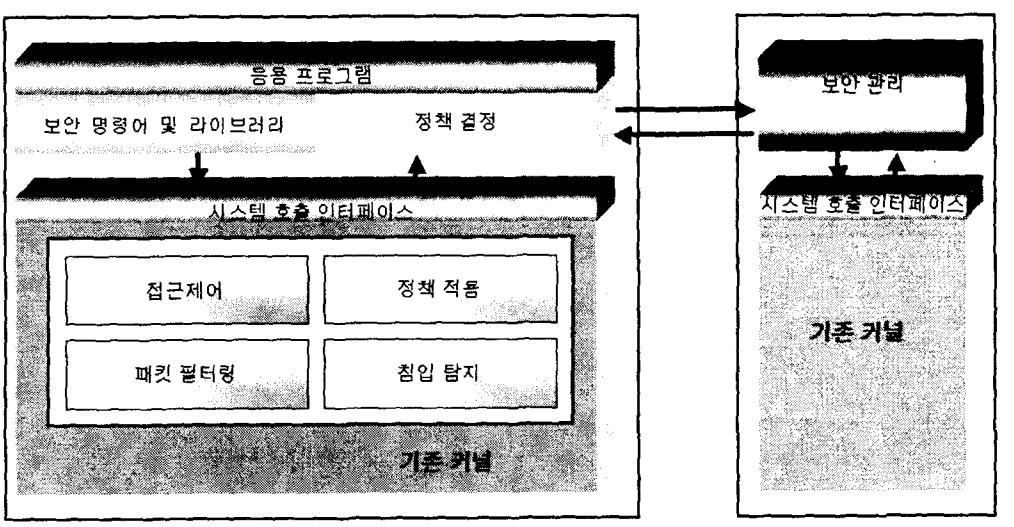

그림 1 네트워 보안 관리 시스템 구성

에서도 보안 관리자 역할이 있어서 보안에 관한 설정 및 운용의 역할을 수행한다. 예를 들어 라우팅 테이블이나 필터링 규칙들을 보안 관리자만이 수정할 수 있도록 해서 루트일지라도 라우팅 테이블을 수정 할 수 없도록 한다. 이렇게 함으로써, 루트권한 획득으로 인한 피해를 최소화 할 수 있다.

3. 침입 대응

네트워을 구성하는 각 라우터나 게이트웨이 등의 네트워 노드들은 보안 기능과 정책 기반 보안 관리가 가능한 기능들을 가지는 secure 노드들로

그림 2 역할기반 접근제어

구성되이 있다. 외부망 또는, 내부 망에 있는 해커들이 네트워을 구성하는 노드들(라우터, 게이트웨이, 스위치 등)을 DoS 공격이나 루트권한 획득을 위해 공격하거나 네트워 내부에 있는 일반 서비스를 제공하는 서버들을 공격하려고 할 때 각 secure 네트워 노드들은 커널 내부에서 침입 탐지 기능을 수행하여 침입이 발견되었을 때, 보안 관리 서버로 침입 사실과 관련 정보를 보낸다. 보안 관리 서버는 각 secure 네트워 노드들로부터 침입 정보들을 수집하고 수집된 정보들에 근거하여 대응 정책을 해당 secure 네트워 노드에 보낸다. 이때의 정책에는 예를 들어 침입된 시스템에서 제공하고 있는 서비스의 세션을 차단하도록 하는 방법과 네트워 노드 자체에서 침입이 오는 소스 주소나 포트 등을 차단하도록 필터링 규칙을 변경하는 정책을 적용하는 방법을 통해 침입지로부터 들어오는 패킷을 거부하도록 하는 방법 등이 있다.

III. 결론 및 향후 과제

본 논문에서는 정책 기반의 네트워 보안 관리 시스템과 네트워 노드 자체에 대한 보안 기능들을 기술하였다. 각 네트워 노드의 커널 레벨에서 동작하는 접근제어 기능, 패킷 필터링 기능, 그리고 침입 탐지 기능들을 통해 침입 정보들을 수집하고 그 수집 정보들을 통해 보안 관리 서버에서는 그에 대응하는 정책을 설정하고 적용하도록 하여 네트워 구성요소 전반의 상호 작용을 통해 네트워 보안을 이룰 수가 있다. 또한, 역할 기반 접근제이를 통한 네트워 노드 자체에 대한 보안을 통해 네트워 노드에 영향을 받은 서브네트워의 보안을 향상시킬 수 있다. 본 시스템에서는 네트워 노드의 커널 레벨에서 침입 탐지 기능, 패킷 필터링 기능들을 제공하도록 하고 있어서 라우터와 같은 네트워 노드에 들어오는 모든 패킷들을 빠짐없이 검사할 수 있다는 장점이 있지만 그에 따른 속도 저하 문제를 고려해야 한다. 앞으로 네트워 노드의 속도 향상 문제에 대해 더 연구를 수행해야 한다.

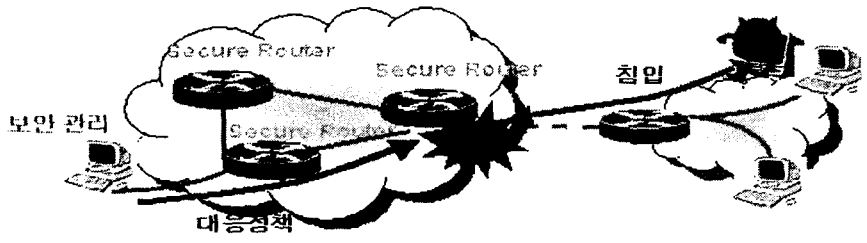

그림 3 침입 대응 방법

참고문헌

[1] Dave Kosiur, "Understanding Policy-Based Networking," WILEY, 2001 년

[2] David F. Ferraiolo, Ravi Sandu, and Serban Gavrila. "A Proposed Standard for Role-Based Access Control", http://csrc.nist.gov/rbac/

[3] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-based Access Control models",IEEE Computer, 29(2):38-47, February 1996.

[4] 조기준, 김훈희, "해킹과 방어 완전 실무", 2001년,