# 보안정책 서버의 경보 데이터 분석 모듈 설계 및 구현+

문호성*, 김은희*, 신문선*, 류근호*, 장종수**
*충북대학교 데이터베이스 연구실
**한국전자통신연구원
e-mail : hsmoon@dblab.chungbuk.ac.kr

# Design and Implementation of Alert Analyzer of Security Policy Server

Ho Sung Moon*, Eun Hee Kim*, Moon Sun Shin*, Keun Ho Ryu*, Jong Su Jang**
*Database Laboratory, Chungbuk National University
**Electronics and Telecommunications Research Institute

요 약

최근 네트워크 구성이 복잡해짐에 따라 정책기반의 네트워크 관리기술에 대한 필요성이 증가하고 있으며, 특히 네트워크 보안관리를 위한 새로운 패러다임으로 정책기반의 네트워크 관리 기술이 도입되고 있다. 보안정책 서버는 새로운 정책을 입력하거나 기존의 정책을 수정, 삭제하는 기능과 보안정책 결정 요구 발생시 정책결정을 수행하여야 하는데 이를 위해서는 보안정책 실행시스템에서 보내온 경보 메시지에 대한 분석 및 관리가 필요하다. 따라서 이 논문에서는 정책기반 네트워크 보안관리 프레임워크의 구조 중에서 보안정책 서버의 효율적인 보안정책 수립 및 수행을 지원하기 위한 경보데이터 관리기를 설계하고 구현한다. 그리고 경보 데이터 저장과 분석을 위해서 데이터베이스 스키마를 설계하고 저장된 경보데이터를 분석하는 모듈을 구현한다. 또한 불량사용자나 호스트의 관리를 위하여 블랙 리스트 매니져를 구현하며 블랙리스트 매니져는 위험한 불량사용자와 호스트를 탐지하여 관리하는 기능을 제공한다. 구현된 경보 관리기나 고수준 분석기는 효율적인 보안정책관리를 지원하게 된다.

## 1. 서론

정책기반의 네트워크 관리는 네트워크 전반에 대해 일관된 정책을 수행하고 적절한 정책을 수립하며, 관리자의 요구에 대해 정책의 용이한 변경을 제공함으로써, 네트워크 전반의 중앙집중적인 관리를 가능케 하는 메커니즘이다[4]. 네트워크 환경에서 동적으로 용이하게 네트워크의 운영 방침을 적용하여 효율적인 네트워크를 운용하는 것이 정책기반의 네트워크 관리의 목적이다. 정책에 의해 운영자는 손쉽게 네트워크를 관리할 수 있으며 상세 구현과 상관없이 일관성 있고 통합적이면서도 이해하기 쉬운 네트워크의 관리를 가능하게 한다. 최근 네트워크 구성이 복잡해짐에 따라 정책기반의 네트워크 관리기술에 대한 필요성이 증가하고 있으며, 특히 네트워크 보안관리를 위한 새로운 패러다임으로 정책기반의 네트워크 관리 기술이 도입되고 있다.

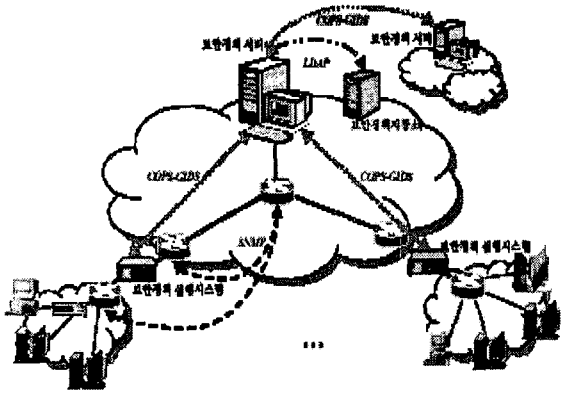
이 논문에서는 정책기반 네트워크 보안관리 프레임워크의 구조 중에서 경보 데이터를 분석하는 부분에 대해 설계하고 구현한다. 논문의 구성은 2장에서는 네트워크 보안제어 시스템의 프레임워크에 대해 간략히 기술한다. 그리고 3장과 4장에서는 경보 데이터를 분석하기 위한 모듈과 불량 사용자 및 호스트 관리 모

+ 이 연구는 한국 과학 재단 RRC (청주대 정보통신 연구센터)의 지원과 ETRI의 연구비 지원으로 수행되었음

듈에 대해 기술하며 5 장에서는 구현을 위하여 모듈을 세부적인 설계한다. 마지막으로 결론 및 향후 연구를 기술하고 끝을 맺는다.

## 2. 관련 연구

정책기반 네트워크 보안구조(Policy-Based Network Management for Network Security: NS-PBNM)는 네트워크 보안을 위한 정책기반의 네트워크 관리 기법으로서 정책기반 네트워크 보안구조를 지칭한다.



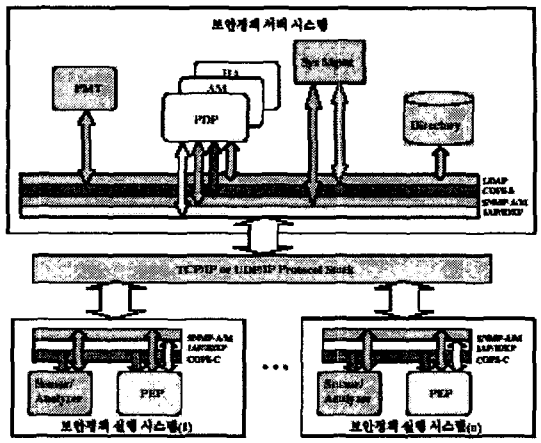
[그림 1] 정책기반 보안 관리의 구성도

정책기반 네트워크 보안관리의 프레임워크의 구성요소는 보안 정책을 생성하고 관리하는 PMT(Policy Management Tool), 보안 규칙에 따라 보안 행위를 결정하는 PDP(Policy Decision Point), 보안 규칙을 저장하는 PR(Policy Repository)와 보안 행위를 수행하는 PEP(Policy Enforcement Point)과 PDP 와 PEP 간의 보안 정책 전달을 위한 통신 프로토콜로 구성된다[5, 6].

네트워크 보안 정책을 위한 프레임은 정책기반 네트워크 보안 구조의 계층적인 구성을 가지며 적어도 두개의 계층으로 구성한다. 하나는 관리 계층에 해당하면 보안 정책 서버 시스템과 다른 하나는 실행 계층에 해당하는 접속점에서의 해킹 트래픽 감지 및 대응을 위한 침입탐지 기반의 보안정책 실행 시스템이다. 보안 정책 서버 시스템은 크게 PMT 블록과 PDP 블록, 보안정책 실행 시스템으로부터 전달된 경보를 처리하는 AM(Alert Manager)과 HA(High-level Analyzer) 블록과 PR 을 위한 디렉토리로 구성된다. 보안 정책 실행 시스템은 네트워크 접속점에서 입력 패킷에 대한 탐지와 분석을 제공하는 Sensor/Analyzer 블록과 보안정책 실행기능을 제공하는 PEP 블록으로 구성된다. 그림 2 는 정책기반 네트워크 보안관리의 구성요소와 상호간의 관계를 나타나고 있다.

## 3. 경보 데이터 분석 모듈

보안정책 서버의 주요 기능 중 하나가 침입이 발생한 경우 보안정책 실행 시스템에서 보낸 경보 메시지에 대한 포괄적이고 광범위한 침입탐지 분석 및 대응 기능이다. 최근의 네트워크 공격은 사전 예측 및 정상 트래픽과의 구분이 어려우며, 그 피해 영역이 단순히 한 시스템이 대상이 아닌 네트워크 전체를 대상으로




[그림 2] 정책기반 네트워크 보안관리의 프레임워크

하고 있다. 이와 같이 네트워크 전방에 걸쳐서 발생되는 침입에 대응하기 위해서는 전체 네트워크에서 발생하는 경보의 포괄적인 분석이 필요하다. 이러한 분석 기능을 제공하고, 다양하고 복잡한 형태의 침입을 탐지하기 위하여 경보 데이터의 상관 관계를 분석하는 모듈이 요구된다.

경보의 상관 관계 분석은 경보 데이터 간의 상호 연관성 추출을 의미한다. 이는 경보의 유사 반복성을 분석하는 유사성 분석과 행위의 상관 관계를 분석하는 행위 분석을 포함한다. 경보의 상관 관계 분석을 위해 요구되는 세부적인 기능은 아래와 같다.

- Repetitive 분석
- Similarity 분석
- Potentiality 분석
- Behavior 분석

Repetitive 분석은 동일한 경보의 반복적인 발생에 대한 분석 기능을 제공한다. Similarity 분석은 동일 근원지 및 목적지에 대해 유사 경보 발생에 대한 분석 기능, 동일 근원지에서 발생하는 유사 경보에 대한 분석 기능과 특정 목적지에 대해 유사 경보 발생에 대한 분석 기능을 제공한다. Potentiality 분석은 잠재적 가능성을 분석하는 기능으로 동일 근원지와 동일 목적지, 동일 근원지, 동일 목적지에 대한 행위에 관련된 분석 기능을 제공한다. Behavior 분석은 경보 시퀀스 분석, 공격 시퀀스 분석, 근원지 시퀀스 분석, 근원지 및 목적지 시퀀스 분석 기능이 포함된다. 경보 시퀀스 분석은 특정 경보 이후에 발생 가능한 경보의 통계적 가능성을 분석하는 기능을 제공한다. 공격 시퀀스 분석, 근원지 시퀀스 분석, 근원지 및 목적지 시퀀스 분석은 특정 공격이나 근원지, 근원지 및 목적지

의 확률적 시퀀스를 의미하며, 기존의 발생 시퀀스를 기반으로 임의의 이벤트 발생시에 다음 단계에서 발생 가능한 이벤트를 확률적으로 분석하는 기능을 제공한다[1, 2, 3].

## 4. 불량 사용자 및 호스트 관리 모듈

불량 사용자 및 호스트 탐지 및 관리 모듈은 보안 서버에 의해 관리되는 영역 내의 침입의 근원지 및 피해 호스트의 체계적인 관리를 제공하는 것이 그 목적이다. 이러한 목적을 위해 경보 데이터를 이용하여 구축된 특정 불량 사용자와 호스트를 감시하고 특별 관리 대상으로 주목함으로써 네트워크의 자원에 대하여 사전 방어 및 조기 대응에 도움을 줄 수 있다.

불량 사용자 및 호스트 관리 모듈은 축적된 경보 데이터로부터 추출된 정보를 가공하여 불량 사용자와 호스트의 리스트를 구축하고 이를 관리하기 위한 관리 모듈(Black List Manager)과 위험한 불량 사용자 및 호스트를 보안 정책에 따라 탐지하기 위한 탐지 모듈(Fault User/Host Function)로 구성이 된다. Black List Manager 는 경보 데이터를 분석하여 불량 사용자와 불량 호스트의 리스트를 구축하고 이를 관리하는 기능을 한다. Fault User/Host Function 은 구축된 불량 사용자와 호스트 리스트를 이용하여 불량 사용자 혹은 호스트의 위험도를 판단하고 정해진 기준을 넘어서는 경우 이를 관리자에게 통보하는 기능을 한다. 이러한 사건의 탐지는 임계 수치를 운용하여 결정하며, 임계 수치는 사용자나 호스트에 대해 총 해킹 건수와 각 임팩트 별 해킹 건수 별로 설정된다. 임계 수치의 값은 관리자의 보안 운용수준에 따라 사전에 학습된 수치를 기준으로 한다.

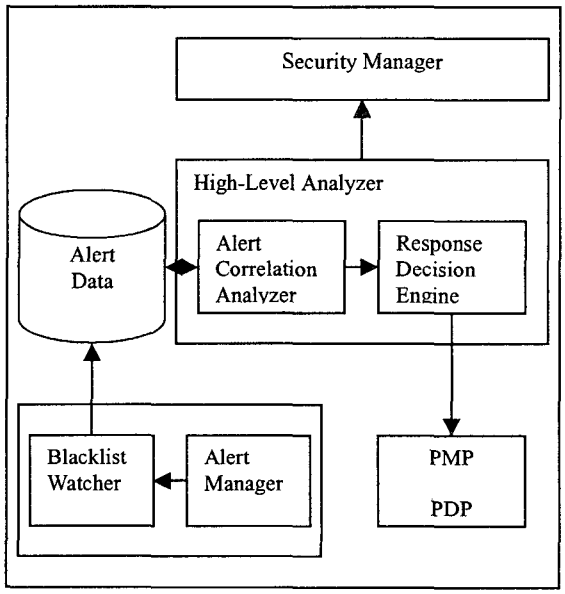
## 5. 구현

보안정책 실행 시스템으로부터 전달되는 침입 정보 등을 구조적으로 저장하기 위하여 보안정책 서버는 RDBMS 를 이용한다. 이는 경보 데이터와 같은 반복적이고 대량의 데이터를 관리하기 위해서는 안정적이고 고속의 RDBMS 가 효과적이기 때문이다. 경보 데이터를 저장하기 위한 스키마는 표 1 과 같다.

보안정책 실행 시스템이 지역적인 침입탐지 메커니즘에 의해 침입이 탐지가 되면 정책에 의한 그 대응과 처리를 수행하고 침입과 대응의 요약 정보를 위의 표 1 의 스키마의 형태로 보안정책 서버 시스템에 전달을 한다. 이렇게 전송된 경보 데이터는 Alert Manager 에 의해 데이터베이스로 구축이 되고, 구축된 데이터베이스의 데이터는 경보 데이터 분석기와 불량 사용자 및 호스트 관리기에 의해 분석되고 관리된다. 분석한 결과에 의해 전체 네트워크에 영향을 미치는 침입이 탐지가 되면 분석기는 그 결과를 보안 관리자와 대응 결정 시스템에 전송을 하고, 이 결과는 정책 결정 과정이나, 침입 대응을 지원하게 된다.

[표 1] 경보 데이터의 구성

| 속성 이름 | 설명 |
|---|---|
| ALID | 경보 데이터 ID |
| SID | 보안정책 실행 시스템 ID |
| ATID | 해킹 ID |
| ATTYPE | 해킹 유형 형태 |
| DDATE | 해킹 탐지 일시 |
| SADDR | 근원지 IP 주소 |
| DADDR | 목적지 IP 주소 |
| SPORT | 근원지 포트 번호 |
| DPORT | 목적지 포트 번호 |
| PROTO | 프로토콜 유형 |
| ICMPTYPE | ICMP 종류 |
| ICMPCODE | ICMP 코드 |
| IMPACT | 임팩트 수준 |
| ACTYPE | 대응 유형 |
| ACRESULT | 대응 결과 |
| ACDATE | 대응 일시 |




[그림 3] 시스템 구성 및 관계

이 논문에서 앞절에서 제시한 경보 데이터의 상관관계 분석을 위해 통계적인 방법을 이용하였다. 설계된 모듈의 지능적인 분석과 탐지를 위해 이후 데이터 마이닝 기법을 응용 및 적용함으로써 고수준의 분석 기능을 제공할 수 있을 것이다. 시스템의 구성과 주변 모듈과의 상관 관계는 그림 3 과 같다.

## 6. 결론

이 논문에서는 보안정책 서버 시스템의 경보 데이터의 상관 관계를 분석하는 모듈을 설계하고 구현하

였다. 또한 침입에 대한 조기 대응이나 사전 방어를 위하여 불량 사용자와 호스트의 리스트를 구축하고 관리하는 모듈을 구현하였다. 축적된 경보 데이터를 분석하여 네트워크 전체에 대한 포괄적인 침입탐지 기능을 제공함으로써 지역적인 침입탐지 시스템에서 탐지가 불가능한 네트워크 전반에 걸친 침입에도 대응하도록 하였다. 현재 우리는 효율적인 경보 데이터의 분석을 위하여 데이터 마이닝 기법을 응용한 분석 방법에 대한 연구를 수행중이다.

## 참고문헌

[1] D.Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition, Hilton Head, SC, Jan. 2000.

[2] D.Schnackenberg, H. Holliday, R. Smith, K. Djahandari, and D. Sterne, "Cooperative Intrusion Traceback and Response Architecture (CITRA)", DISCEX'01, Anaheim, California, June. 2001.

[3] S. M. Lewandowski, D. J. Van Hook, G. C. O'Leary, J. W. Haines, and L. M. Rossey, "SARA: Survivable Autonomic Response Architecture", DISCEX'01, Anaheim, California, June. 2001.

[4] IPHIGHWAY, Inc., "Introduction to Policy-based networking and Quality of Service", http://www.iphighway.com.

[5] E. Lupu and M. Sloman, "Conflicts in Policy-based Distributed Systems Management", IEEE Transactions on Software Engineering, Vol. 25, No. 6, Nov. 1999.

[6] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, and S. Waldbusser, "Terminology for Policy-Based Management", IETF <draft-ietf-policy-terminology-04.txt>, July 2001.

[7] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen, "Policy Core Information Model – Version 1 Specification", IETF RFC3060, Feb. 2001.

[8] M.Wahl, T.Howes, S.Kille, "Lightweight Directory Access Protocol (v3)", IETF RFC 2251, Proposed Standard, Dec. 1997.

[9] J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service Protocol", IETF <draft-ietf-rap-cops-07.txt>, Aug. 1999.

[10] P. Ferguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", IETF RFC2827, May. 2000.