2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

광역망에서의 정책기반 보안프레임워크

박상길*, 장종수*, 노봉남**
*한국전자통신연구원 정보보호연구본부
**전남대학교 전산학과
e-mail : wideideal@etri.re.kr

A Policy based Secure Framework In WAN

Sang-Gil Park*, Jong-Su Jang*, Bong-Nam Noh**
*Information Security Division, Electronic Telecommunication Research Institute
**Dept. of Computer Science, Chon-Nam University

요 약

인터넷의 지속적인 보급/발전과 더불어, 네트워크 상에서의 침입시도는 해가 지날수록 기하급수적으로 증가되고, 그 기법또한 다변화되고 있다. 이는 침입탐지시스템의 적용환경에도 많은 영향을 끼치게 되었다. 일반적인 네트워크 기반 침입탐지시스템은 네트워크 디바이스를 통해 유입되는 패킷에 대해 Signature 기반 침입탐지 모듈을 통하여 침입을 탐지하게 된다. 대게의 경우 새로운 침입탐지 패턴이 생성되었을 경우, 사용자에 의해 추가되거나 또는 소스코드의 재컴파일을 통하여 시스템이 재구동되기도 한다. 본 논문이 제시하는 바는 이에 반해 AS 내에 존재하는 네트워크의 유입점인 게이트웨이 장치에 침입탐지 시스템을 설치하며, 이를 보안정책서버에 의해 정의된 정책에 의해 침입탐지 및 게이트웨이 장치로서 동작하게 한다. 이를 통해 보안정책서버에 추가되는 침입탐지 패턴등의 정책정보가 각 침입탐지시스템에 실시간으로 반영되어 처리된다.

1. 서론

침입탐지 시스템(IDS)은 침입이 발생할 때 탐지하는 보안 메커니즘이다. 전통적인 침입탐지 시스템의 설계방법의 한계점으로 다음과 같은 사항이 있다.

- 모니터되는 시스템의 크기 증가로 확장이 어렵다.
- 한 곳에서 모든 것을 관리하여 IDS 를 취약하게 만든다.
- IDS 기능 추가와 재구성이 어렵다.

본 논문에서는 중앙정책제어서버로부터의 정책을 네트워크 유입단인 보안게이트웨이 시스템의 침입탐지 모듈에 적용하여 침입탐지를 수행하며, 네트워크 유입단에 설치된 게이트웨이에 보안정책의 업데이트를 통하여 변경된 보안정책을 수행하는 방법에 대하여 기술하고자 한다.

2. 관련연구

2.1 침입탐지 및 대응기술

침입탐지 시스템(IDS : Intrusion Detection System)은 외부로부터 허가되지 않은 접근이나 해킹을 감지하여 시스템 및 망 운영자에게 통보하여 주고, 필요한 대응을 취하는 시스템을 말한다. 여기에서 허가되지 않은 접근이나 해킹은 내, 외부 침입자에 의한 비정상적인 사용(Anomaly), 오용(Misuse), 남용(abuse) 등이 모두 포함된다. 일반적으로 침입탐지 시스템은 실시간에 시스템에 관한 정보나 네트워크상의 패킷으로부터 획득한 정보를 사용하거나 감사 기록(Auditing Log Data), 시스템 테이블, 네트워크 트래픽 기록 등으로부터 사용자 행위(Activity)에 대한 정보를 분석하여 침입이 발생했는지의 여부를 판단한다.

IDS 는 사용호스트에서 감시 S/W 로 존재하거나, 네트워크에 연결하여 네트워크 트래픽을 감시하는 형태 또는 양쪽 모두의 형태를 이용한다. 네트워크 기반 IDS 는 호스트마다 설치하여야 하는 부담이 없고 다양한 형태의 공격에 대한 감시가 가능한 반면, 호스트 기반 IDS 는 특정 호스트에만 적용되지만 내부 사용자의 허가되지 않은 행위와 응용계층 프로토콜에 대한 감시 등 비교적 자세한 감시가 가능하다.

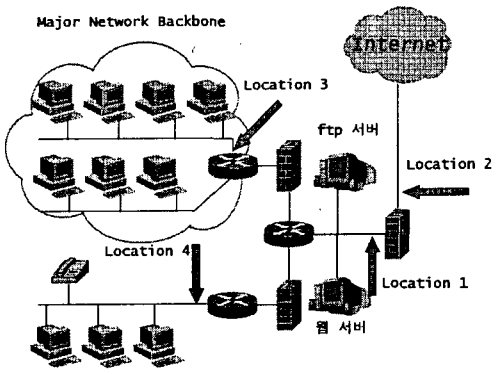

그림 1 침입탐지시스템의 배치

침입탐지시스템의 배치에 따라 다음과 같은 기능을 수행할 수 있다.

Location 1 의 경우
- Network 방어선을 관통하는 외부 공격을 인지
- Network 방화벽의 정책과 성능을 부각
- DMZ 내의 Web Server 나 ftp server 의 공격을 알 수 있음
- Outgoing Traffic 인지 가능

Location 2 의 경우
- Internet 을 통한 network 공격의 수와 형태를 문서화 가능

Location 3 의 경우
- Attack 발견 가능성 증가
- 보안 경계선 내에서의 인증된 사용자의 인증되지 않은 Activity 탐지

Location 4 의 경우
- System 과 Resource 공격 탐지

이러한 침입탐지 시스템에서 사용되고 있는 기존의 기술들은 접근 통제기술, 취약점 탐지 기술, 패킷 캡처기술, 정보가공 및 축약 기술, 침입탐지 정보에 대한 통계적 분석 기술, 실시간 대응/보고 기술, 새로운 침입패턴 생성 기술 등이다.

2.2 정책기반 망관리

정책기반의 망 관리구조는 IETF 에서 그림 1 과 같이 정책관리를 위한 Policy Management Tool(PMT), 정책 저장을 위한 Policy Repository, 정책 결정을 위한 Policy consumer(Policy Decision Point : PDP), 정책 적용을 위한 Policy Target(Policy Enforcement Point : PEP) 등의 기능적 구성 요소로 표현 가능하다.

망관리에 관한 정책은 정책 저장소(Policy Repository)에 저장되며, 망 내부의 분산되어 있는 정책 결정부(PDP)에 의해 실시간으로 검색된다. 정책 데이터는 Policy Condition 과 Action 으로 구성되며, 효율적인 보안정책의 적용을 위해 Policy Rule 과 Group 등의 데이터 스키마를 제공한다.

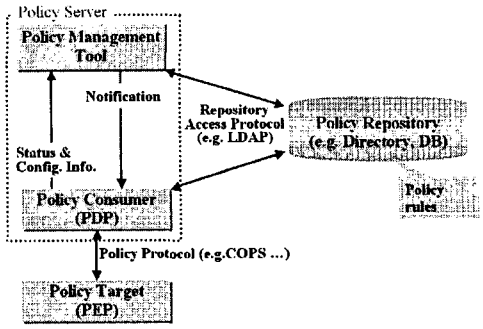

그림 2 IETF 의 정책기반 망 관리구조

정책을 조회하거나 신규 생성된 정책을 저장하는 프로토콜로는 디렉토리 서비스에 사용되는 LDAP (Lightweight Directory Access Protocol)v3 가 사용된다. 정책기반 네트워크 관리구조에서 Policy Rule 은 "If (condition), Then (Action)"의 형태로 생성되며, 이러한 Policy Rule 은 Policy Repository 에 변환되어 저장되며, 운영자에 의해 Target(PEP)에 적용된다.

2.3 정책 전달 프로토콜

정책기반 망관리(Policy Based Network Management)는 네트워크 환경에서 동적으로 네트워크의 운영방침을 적용하여 효율적인 네트워크를 운영하는데 그 목적이 있다. 이를 위한 정책을 전달하기 위하여 기존의 망관리 프로토콜인 SNMP(Simple Network Management Protocol)와 실제 정책 전달을 위하여 설계된 COPS(Common Open Policy Service)를 사용한다.

COPS 는 PDP 와 PEP 사이에서 Client/Server 모델로서 사용되며 request/response 방법으로 동작된다. COPS 는 TCP connection 을 이용하며, 모든 COPS 메시지는 common header 로 시작하고, Header 는 8 비트, Op Code 로 10 개의 operation 의 정의가 가능하다.

COPS 는 아래 그림 3 과 같은 구조를 갖고, 망에 제공된다.

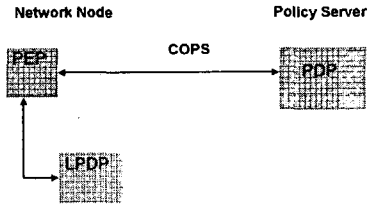

그림 3 COPS 기본구조

3. 정책기반 보안프레임 워크

보안정책 규칙은 보안 정책 시스템의 핵심으로서 개체들 사이에서 상호 운용성을 나타내며 Condition/Action 으로서 표현되어진다. 계층적 구조를 갖는 보안정책 모델은 다음과 같다.

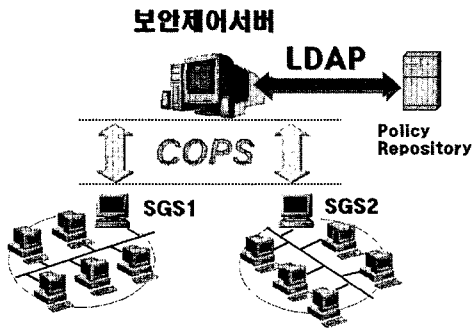

그림 4 정책기반 보안프레임워크

정책기반 보안프레임워크는 계층적인 구조이며 적어도 2 개의 계층으로 구성된다. 하나의 계층은 관리계층이며 PMT 의 기능과 PDP 의 기능을 담당하는 보안제어 서버로서의 역할을 담당하게 된다. 다른 하나의 계층은 실행계층으로서 네트워크의 접속점에 위치하게 되며, 해킹 트래픽 탐지 및 대응을 위한 침입탐지시스템 기반의 보안게이트웨이 시스템(SGS : Security Gateway System)이다. 보안제어서버와 SGS 간의 정책의 전달은 COPS 를 통하여 전달되며, Policy Repository 와 PMT 간의 정책자료의 전달은 LDAP 을 이용하여 전달되며, SGS 와 보안제어서버와의 구성관리는 SNMP 를 이용하여 운용된다.

보안제어서버의 PMT 는 SGS 에서 적용할 Policy 를 생성하여 LDAP 을 이용하여 Policy Repository 에 저장한다. 보안제어서버의 PDP 는 Plicy Repository 에 저장된 정책 정보를 읽어와서 SGS 가 이해할 수 있는 데이터스키마 체계로 변환 한 후 SGS 내부에서 PEP 기능을 담당하는 CP-A 에게 전달하면, CP-A 는 추가되는 침입탐지 패턴 정보등을 SGS 내부의 RDBMS 에 update 한 후, Analyzer 에 통보하여 추가된 침입패턴에 대한 침입탐지를 수행하게 한다.

이때 PMT 가 정의하는 Policy 에 관한 정보는 DMTF 에서 추진중인 CIM 을 이용하여 modeling 을 하였고, 이 Policy 정보는 LDAP 프로토콜을 이용하는 Policy Repository 에 저장되기 위하여 LDIF 형식으로 변환되어 저장된다. 보안제어서버의 PDP 는 관리대상에 적용하고자 하는 정책을 LDAP 프로토콜을 이용하여 Policy Repository 에 조회한 후 해당 정책 데이터를 ASN.1 형식의 PIB 로 변환하여 SGS 에 내려준다.

SGS 내부에서 PEP 기능을 수행하는 CP-A 는 수신된 PIB 를 해독하여 SGS 내부에서 침입탐지 패턴용 DB 에 맞는 스키마로 변환하여 저장한다. 그후 CP-A 는 침입탐지 기능을 수행하는 Sensor/Analyzer 에게 Update 된 보안정책을 적용하여 침입탐지기능을 수행하도록 정보를 전달한다.

위 기법을 이용하여 관리대상에 대하여 통일된 보안정책의 수행이 가능하며, 새로운 유형의 Attack 이 발견되더라도 시스템에 영향을 끼치지 않고 on-line 상 update 가 가능하다.

3.1 보안제어서버

보안제어서버는 보안게이트웨이 시스템에 의해 명백히 침입이라고 판정되지 않는 suspicious data 를 분석(analyze)한다. 보안제어서버는 침입탐지 정책의 구성에 관해 관리자(Administrator)에 의해 요구를 받는다.

보안제어서버는 보안게이트웨이 시스템으로부터 Event Log 데이터를 수신받아 주기적으로 통계적인 정보를 생성해낸다. 이러한 정보를 기반으로 보안게이트웨이 시스템 단에서 침입이라고 단정하기 어려운 event 에 대하여 High Level Analyzer 를 통하여 침입을 탐지하게 된다. 보안제어서버의 High Level Analyzer 는 Event Log 데이터와 보안게이트웨이 시스템(SGS : Security Gateway System)으로부터 전송되는 침입에 대한 경보메시지를 이용하여 가공작업을 통하여 침입탐지를 수행하게 된다.

보안제어서버의 세부 기능으로는 다음과 같다.

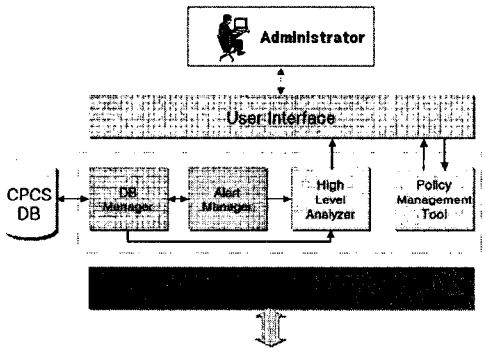

그림 5 보안제어서버의 기능 블록도

- Administrator : 보안프레임워크 전체에 대한 관리의 책임이 있으며, 침입에 관련된 정보를 User Interface 를 통하여 수신하며, 그에 적절한 대응을 취하도록 지시.
- User Interface : Administrator 로부터의 모든 요청 메시지등을 처리하며, Alert Manager 로부터 발생되는 보안 경보메시지를 Administrator 에 전달.
- DB Manager : CPCS DB 뿐만 아니라 User Interface Table, SGS Table, Policy Table, System Log 등을 제어.(필요할 경우 event log profile table, alert log profile table, TCP session table 과 UDP/ICMP 패킷 정보 table 등을 제어).
- Alert Manager : SGSs 로부터의 침입경보메시지를 수신하여 High Level Analyzer 에 전달 및 침입경보메시지 가공
- High Level Analyzer : Coordinated Attack 탐지와 Anomaly 탐지를 위한 보안제어서버의 핵심기능으로서, 보안제어서버상의 시스템의 침입도 탐지하며, Alert Manager 로부터의 경보데이터와 TCP Session 정보등을 이용하여 네트워크 전반에 걸친 Attack 을 탐지.
- Policy Management Tool : SGSs 에서 사용되는

Pattern 에 관련된 정책을 결정한다. Administrator 로부터 망 전체에 대한 정책을 전달받아 관리대상 객체인 SGSs 에 적용.

- COPS Server : COPS 프로토콜을 통하여 정책을 송수신하는 기능.

3.2 보안게이트웨이 시스템

보안게이트웨이 시스템(SGS : Security Gateway System)은 네트워크의 유입지점인 게이트웨이 역할을 수행하는 라우터 상에서 네트워크 기반 침입탐지 역할을 수행하는 Sensor/Analyzer 를 탑재하고, COPS Client 를 통하여 수신된 정책정보에 의하여 침입을 탐지하며, 탐지된 각각의 침입에 대하여 CP-A 를 통해 Alert Message 를 조합한 후 COPS Server 를 통하여 보안제어서버에 전달한다.

보안게이트웨이 시스템이 탐지하는 방법은 네트워크 기반 침입탐지를 수행하며 Misuse 방법을 사용한다. 새로운 유형의 Attack 의 추가가 필요할 경우 보안제어서버에서 COPS Client 에 전달하면 CP-A 는 PIB 형태로 수신된 정책정보를 RDB 스키마에 맡게 변환한 후 Analyzer 에게 패턴정보의 업데이트 메시지를 전송하여, Analzyer 가 재구동이 필요없이 메모리상에 추가된 패턴정보를 로딩하여 새로운 유형의 Attack 에 유연하게 대응한다.

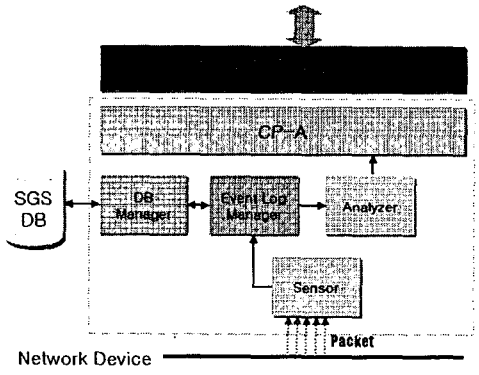

그림 6 보안게이트웨이 시스템의 기능 블록도

그림에서 보는 것처럼 SGS 는 크게 4 가지의 구성요소로 구분되어 진다.

- COPS Client : 보안제어서버와의 정책 송수신 및 Alert Data 등의 전송경로로 사용
- CP-A : SGS 의 DB Management 와 SGS 내에서의 PEP 기능의 수행 및 Local PDP 기능 수행.
- Sensor/Analyzer : 네트워크로부터의 패킷의 유입시 패킷을 수집, 축약, 캡춰 한 후 정해진 보안정책(침입탐지 패턴)에 의해 침입을 탐지한다. Sensor 로부터 생성된 Event Log Data 는 일정기간마다 ftp 경로를 통하여 보안제어서버에 전송된다.
- DB Manager : 보안정책(침입탐지 패턴)및 SGS 구성관리 table, Event Log table, Alert table 등을 관리한다.

4. 정책기반 보안프레임워크의 장점

정책기반 보안프레임워크의 가장 큰 장점은 망 전체가 통일된 정책하에 침입을 탐지하며, 침입을 차단할 수 있는 기능을 제공하게 되는 것이다. 또한 SGS 에서는 네트워크 기반의 침입탐지 패턴에 의해 misuse 탐지를 수행하며, SGSs 들에 의해 확실히 침입으로 판명되지는 않지만, Alert Messae 와 TCP Session Log 등의 Data 를 이용한 High Level Analyzer 를 이용하여 Anomaly Detection 과 Coordinated Attack 을 탐지할 수 있다.

본 논문에서는 2 개의 계층구조로서 보안프레임워크를 구성하였으나, 보안제어서버를 제어하는 최상위 보안제어서버를 통하여 WAN 영역에서도 일괄된 보안정책하에 네트워크를 통하여 유입되고 유출되는 네트워크 패킷에 대하여 침입탐지를 원활히 수행가능하다.

5. 결론 및 향후과제

네트워크 기반 침입탐지시스템기술의 핵심은 유입되는 패킷을 유실하지 않고 캡춰링하며, 시도되는 공격에 대하여 적절한 대응을하는 것이다. 그러나, 네트워크에 유입되는 패킷이 처리할 수 있는 능력보다 많을 경우 네트워크 기반 침입탐지 시스템이 원활히 동작하리라 보장하기는 힘들다. 따라서, 본 논문이 제시하였던 내용 중 SGS 의 Sensor 의 기능을 Embedded 화 하여 하드웨어 수준에서의 패킷의 캡춰링과 축약 등의 작업이 수행되면, 이더넷 뿐만 아니라 기가 이더넷과 백본망에서도 정책기반 네트워크침입탐지를 수행하는 프레임워크로 동작될 것이다.

참고문헌

[1] D. E. Denning, "An Intrusion-Detection Model", In *proceedings of the IEEE Symposium on Security and Privacy*, pp.118-131, 1986

[2] S. Northcutt, M, Cooper, M. Fearnow, K. Fredrick, *Intrusion Signature and Analysis*, new Riders, 2000.

[3] Rebecca Bace, Peter Mell, "Intrusion Detection Systems", Aug. 2001. http://csrc.nist.gov/publications/ nistpubs/800-31/sp800-31.pdf

[4] *Introduction to Policy Based Networking & QoS*, White paper, http://www.iphighway.com

[5] RFC 2753, *"A Framework for Policy-based Admission Control"*, Jan. 2000.

[6] RFC 2401, *"Security Architecture for the Internet Protoco"*, Nov. 1998.

[7] RFC 2748, "The COPS(Common Open Policy Service) protocol", Jan, 2000

[8] RFC 2251, "Lightweight Directory Access Protocol(v3)", Dec, 1997.