이기종 IDS 환경에서 효과적인 침입탐지를 위한 통합패턴 모델

김찬일*, 김상호*
*한국정보보호진흥원
e-mail : chankim@kisa.or.kr, shkim@kisa.or.kr

Integrated Pattern Model for Intrusion Detection under Heterogeneous IDS Environment

Chan-Il Kim*, Sang-Ho Kim*
*Korea Information Security Agency

요 약

다양한 위협과 침입공격에 노출되어 있는 조직의 경우, 특정 제품에서 제공하는 한정된 침입탐지패턴의 한계를 극복하여 침입사건을 효과적으로 탐지하여 대응하기 위하여 이기종 침입탐지시스템 설치 및 운용이 요구된다. 이기종 침입탐지시스템 운용은 침입탐지 감사데이터 포맷이 제품별로 상이하고, 두개 제품 이상에 구현된 동일한 침입탐지 패턴이라도 설계의 차이점에 기인하여 오판률 가능성이 증가할 가능성이 있으며, 특히 탐지사건에 대한 대응으로 e-mail, SMS 등을 이용할 경우 중복 탐지로 인한 과도한 대응 등의 문제점이 있을 수 있으므로 이기종 침입탐지시스템 운영 환경에 적합한 기종간 통합 및 대응 모델과 관련 모듈 설계에 관한 연구가 필요하다. 본 논문에서는 최근 연구되는 Aggregation 및 Correlation 개념을 적용하여 이기종 침입탐지시스템 운용 환경에서 침입탐지패턴 통합 및 대응을 위한 요구사항을 도출하고 통합 및 대응을 위한 IPMAC 모델 및 탐지알고리즘을 제시하여 관련 모듈을 설계 및 구현한 결과를 제안한다.

1. 서론

인터넷 등 개방형 네트워크를 통하여 내외부 불법 공격자의 정보시스템의 취약점을 이용한 침입공격으로 인한 피해가 빈번해 짐에 따라 침입탐지시스템은 침입을 사전에 탐지하여 대응하여 피해를 최소화하는 대응책으로서 유용성과 그 가치가 인정되어 정보보호의 중요한 기술 요소로서 인식되고 있다[1]. 최근에 침입탐지시스템은 복합적인 침입패턴에 대한 탐지의 어려움, 침입탐지 오판가능성 등 한계 점에 하고 있다. 이러한 한계점 극복을 위하여 2 개 이상의 침입탐지시스템을 분산 배치하여 탐지기능을 향상 시키는 분산 침입탐지시스템 관련 연구와 분산 시스템의 침입탐지 경보를 수집 및 침입 관련 정보를 연계하여 복합적인 침입여부를 결정하는 AC(Aggregation and Correlation)연구[2][3][4][5][6]가 활발하게 진행되고 있다.

AC 는 대량의 침입경보 발생, 유사공격을 알려 주지 못하는 점, false Alerts 발생, scalability 의 문제점 등 침입탐지시스템의 문제점을 해결할 수 있다.[2]. 그러나 이런 연구는 침입경보를 발생하는 침입탐지시스템의 신뢰성에 의존하므로 보안정책 설정의 잘못이나 잘못된 침입경보로 인한 문제점이 있다. 본 논문에서는 기존 AC 관련 연구에, 이기종 침입탐지시스템 환경에서 에이전트를 설계 및 각 시스템에 설치하여 능동적으로 침입탐지패턴을 통합하는 모델을 제안한다.

2 장에서 관련 연구를 정리하고, 3 장에서 사전 요구사항 및 조건을 도출한다. 4 장에서 통합 모델로서 IPMAC 을 설계하고 구현한 결과를 제시한다. 5 장에서는 향후 연구과제 및 결론을 제시한다.

2. 관련 연구

AC 는 최근 연구되는 복수개 침입탐지시스템의

Alert 를 분석하여 중복된 경보를 제거, 유사한 공격의 그룹화, false Positives or false negatives 감소와 계층적 구조로 배치하여 Load 를 분산하여 관리자에게 최적의 경보를 알려 주는 시스템 설계를 위한 요소이다 [2][3]. 그림 1 은 AC 를 이용한 시스템의 구조로서 다음과 같은 분류를 고려하여 다양하게 연구 되고 있다.

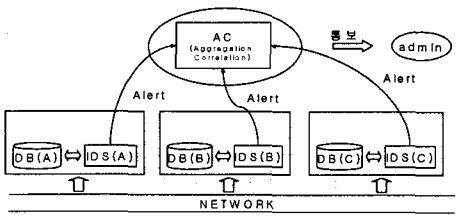

그림 1 Aggregation and Correlation for IDS Alert

(1) 운영 체제 기반 분류
- o 같은 기반의 종류와 이기종 IDS 의 Alert 수집
- o 다른 기반의 종류와 이기종 IDS 의 Alert 를 수집
- o 두개를 합쳐서 적절하게 사용하는 방법

(2) 침입관련 타입 분류
- o 싱글 센스와 다중 센스 방법
- o real time 과 affer-the-fact
- o in-band 와 all-band 방법

(3) 침입결정 방식 분류
- o 통계적 방법- 임계값 이상으로 Alert 의 개수 통보 받으면 침입으로 간주하는 방법
- o 가중치 적용 방법 – 침입탐지시스템의 Alert 의 가중치를 두어 결정하는 방법
- o 무조건 선택하는 방법 – 한 개라도 Alert 가 오면 침입으로 결정하는 방법

3. 통합패턴 모델(IPMA)의 사전요구사항 및 조건

기존의 AC 구조는 각 침입탐지시스템의 Alert 을 받고 이 Alert 을 분석하여 탐지여부를 결정하는 중복 및 유사한 Alert 으로 인한 탐지 오판율이 발생하는 문제가 있으므로 본 논문에서는 탐지의 정확성을 이고 탐지 오판율을 최소화하기 위하여 기존 AC 시스템에 에이전트를 설치하여 각각의 침입탐지시스템의 침입탐지패턴을 수집하여 데이터베이스로 구축하고 침입탐지 여부를 결정하는 모델을 제시 하고자 한다.

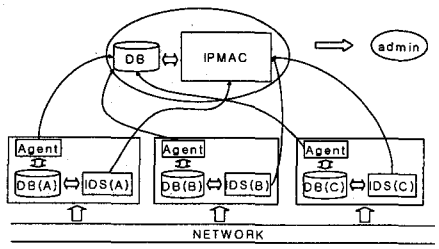

그림 2 Integrated Pattern Model for AC

IPMAC 설계를 위해서는 설계 전에 선행 되어야 할 요구사항과 조건이 있다. 다른 포맷형식으로 된 침입탐지패턴을 IPMAC 에서 통합 그룹화하기 위해서는 어려움이 있으므로 이런 어려움을 해결하기 위해서는 다음과 같은 조건 중 한 개 이상을 만족해야 한다. 첫째, 각각의 침입탐지시스템의 데이터베이스를 포맷을 통합하여 표준 포맷으로 통일하는 방법, 둘째, 침입탐지시스템 업체에서 제공하는 침입탐지패턴 항목 중 최소한의 필요한 데이터 항목을 얻을 수 있는 함수를 제공하는 방법, 마지막으로 중간 미들웨어 두어 IPMAC 업체와 침입탐지시스템의 개발자 업체로부터 독립 될 수 있는 미들웨어 제품을 제공하는 방법이 있다.

본 논문에서는 데이터베이스에 접근할 수 있는 공개함수 제공된다는 가정 하에서 사전 요구사항을 정의한다.

(1) 데이터베이스를 접근할 수 있는 계정과 패스워드를 미리 획득한다. 이 계정은 데이터를 얻을 수 있으며 삽입/삭제 기능이 제공되지 않는다.

(2) IPMAC 과 에이전트 통신은 허가된 사용자만 통신할 수 있도록 인증 절차가 수행되어야 한다.

(3) IPMAC 과 에이전트 통신은 안전하게 통신할 수 있도록 안전한 경로가 제공되어야 한다.

(4) IPMAC 과 에이전트 통신 중 IPMAC 에게 정확한 정보가 제공할 수 있도록 비밀성이 제공 되어야 한다.

4. IPMAC 의 설계 및 구현

본 장에서는 IPMA 의 기본 구조와 세부적인 모듈로 분리하여 설계 및 구현한 결과를 제안한다.

(1) 기본 구조

o 데이터 수집 모듈

IPMAC 은 서버에 위치하여 데이터를 분류하는 Data Classifier 모듈과 각 침입탐지시스템의 운영체제에 위치하여 침입탐지패턴을 수집하는 Agent 모듈로 나누어진다.

데이터 수집 모듈은 그림 3 과 같은 구조를 가지게 된다.

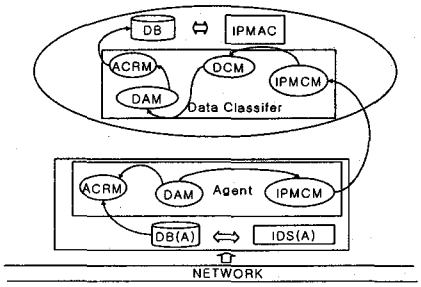

그림 3 데이터 수집 모델의 세분화

IPMCM(IPM Communication Module) : IPMAC 의 data Classifer 와 Agent 사이의 통신을 위한 모듈.

DCM(Data Classify Module) : 각 에이전트에서 받은

침입탐지패턴을 분류하는 작업을 한다.

DAM(Data Access Module) : 데이터 베이스에 접근하기 위한 모듈로써 각각의 이기종 침입탐지시스템에서 제공하는 함수를 이용하여 데이터베이스에 접근한다.

ACRM(AC Read Module) : 각각의 이기종 침입탐지시스템 업체에서 제공하는 함수를 이용하여 데이터베이스에서 데이터를 읽어오는 모듈이며 이것은 침입탐지시스템 업체에서 제공한다.

ACWM(AC Write Module) : 침입탐지패턴을 수집한 데이터를 데이터베이스에 저장하는 모듈이다.

o IPMAC 모듈 구조

IPMAC 모듈의 구조는 다음과 같다. IPMAC 에 자체 침입탐지시스템 능력이 추가된다. 그렇지만 자체 침입탐지시스템이 모든 공격을 탐지하는 것은 아니다. 이것은 단순히 수집된 침입탐지패턴과 비교하는 기능만을 수행하며, 복잡하고 Load 가 많이 걸리는 침입은 탐지 하지 않고, 침입탐지 하기 위한 보조 또는 확인 작업으로만 사용된다.

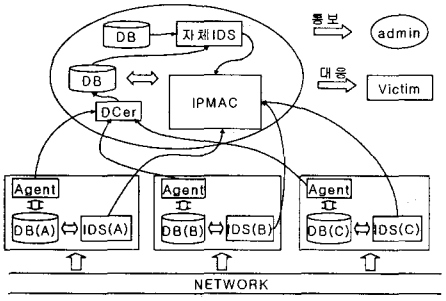

그림 4 IPMAC 세분 모듈 구조

IPMAC(Integrated Pattern Model for AC) : 기존 AC 에서 받은 Alert 와 자체 침입탐지시스템에서 받은 Alert 및 각각의 이기종 침입탐지시스템의 침입탐지패턴을 받아 AC 알고리즘으로 침입여부를 결정하는 모듈이다.

DCer(Data Classifier Module) : 각 침입탐지시스템에 있는 에이젼트에서 받은 데이터를 분류 그룹화하여 데이터베이스에 저장하는 모듈로서 각각의 세부 모듈을 모두 합쳐 있는 상위 레벨의 모듈이다.

ACRM(AC Read Module) : 제공하는 함수를 이용하여 데이터베이스에서 데이터를 읽어오는 모듈이다.

(2) IPMAC 모델 설계

IPMAC 을 설계하기 위해서는 먼저 데이터 포맷을 정해야 한다. 모든 데이터 항목을 침입탐지패턴으로 구축하기 어렵기 때문에 침입탐지시스템에서 공통으로 사용할 수 있는 침입탐지패턴 데이터 요소를 분류 및 그룹화한다. 또한 침입탐지패턴 데이터 항목 외에 IPMAC 에서 사용되는 분류코드와 침입탐지시스템코드를 추가하여 데이터 베이스를 구축한다.

o IPMAC 의 침입탐지패턴 포맷

침입탐지시스템은 제품특성, 구현 언어, 처리 능력 등을 고려하여 각각의 형태로 침입탐지패턴을 구성한다. 각 이기종 침입탐지패턴을 통합하고 분류하여 IPMCA 에서 사용 적합한 포맷으로 변경 한다.

본 논문에서 제시한 데이터 포맷 항목은 꼭 필요한 최소의 항목만을 기술한 것이다.

표 1 수집되는 최소 침입탐지패턴 포맷

인덱스	패턴 내용	포트	분류코드	침입탐지시스템코드

표 2 IPMAC 에서 분석하기 위한 최소 Alert 포맷

패턴 내용	포트	소스	목적	분류 코드	침입탐지시스템코드	시간

표 3 IPMAC 의 최소 침입탐지패턴 포맷

인덱스	패턴 내용	포트	분류 코드	침입탐지시스템코드	가중치	재분류 코드

- 인덱스: 유일한 번호를 가지고 식별하기 위한 번호
- 패턴내용: 침입 여부를 비교하는 침입탐지패턴 내용
- 포트: 침입탐지 여부를 비교시 이용되는 포트 번호
- 분류코드:침입탐지패턴을 분류 또는 그룹화 시 식별하기 위한 번호
- 침입탐지시스템코드: 각각의 업체의 식별하는 번호
- 가중치: 침입탐지시스템코드의 가중치 값이 설정됨
- 재분류코드: 임시코드나 분류코드를 다시 재정의

o IPMAC 의 침입탐지패턴 구축

분류코드가 있으며 동일한 인덱스일 경우, 동일한 침입탐지패턴을 인식하고 같은 분류코드 번호를 가지면 유사한 침입탐지패턴으로 인식한다. 다음으로 고려할 점은 침입탐지시스템코드로 각각의 가중치를 분류코드 기준으로 두어 각 침입탐지시스템의 탐지 여부를 결정한다. 만약 분류코드가 없으면 임시 분류코드를 부여하고 저장한다. 그리고 관리자가 임시코드를 분류코드에 포함 시킬 필요가 있을 때 재분류코드에 분류코드 값을 사용한다. 즉 임시로 받은 코드는 관리자가 침입탐지패턴을 적당하게 분류하여 저장하는 것이다.

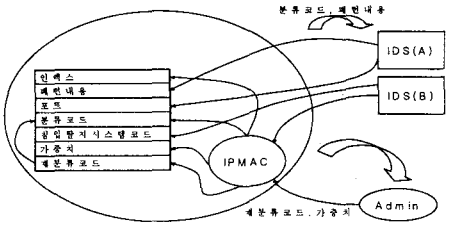

그림 5 IPMAC 침입탐지패턴 구축

o 가중치를 고려한 탐지 알고리즘

각각의 침입탐지시스템은 침입탐지패턴에 대하여 가중치를 둔다. 각각의 침입탐지시스템은 가장 잘 탐지하는 패턴에 대하여 가중치를 두어 좀더 정확한 탐지를 한다. 가중치에 의한 탐지 결정 방법은 표 4 에 따라 결정 된다.

표 4 다중 탐지 시 IPMAC 탐지 결정 테이블

침입탐지 패턴	IDS(A) (high)	IDS(B)	자체 IDS(A)	패킷 분석	공격 여부
A, B	o	o	-	-	o
A, B	o	x	-	-	o
A, B	x	o	o	-	o
			x	o	o
				x	x
A, B	x	x	o	o	o
				x	x
			x	-	x

분류와 그룹화된 침입탐지패턴은 false Positive 와 false negative 를 줄인다. 기존의 AC 기능에 각 침입탐지시스템에서 가지고 온 침입탐지패턴과 Alert 를 비교하고 침입탐지패턴을 그룹화하여 중복된 탐지를 줄이고 유사한 탐지를 그룹화 하여 사용자에게 유용하게 알려 준다. 여기서 사용되는 패킷 분석 기능은 각 침입탐지시스템에 온 Alert 로 침입탐지를 결정하기 불투명할 때 패킷분석을 정확히 하도록 요청하는 것이다.

(3) IPMAC 모델 구현

이기종 침입탐지시스템은 각각의 다른 운영체제에서 시스템이 동작하고 침입탐지시스템에 따라 각각의 다른 데이터베이스를 사용하기 때문에 구현하기가 쉽지 않지만, 여러 가지 기술을 사용하여 구현 할 수 있다.

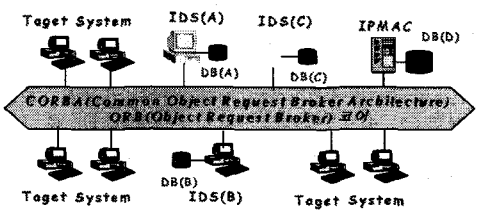

그림 6 IPMAC 구축 시스템 환경

본 논문에서 구현된 시스템은 Widow 2000 Pro 에서 동작하는 침입탐지시스템 2 개와 침입탐지패턴을 저장하는 데이터베이스로 Oralce 과 MS Access 를 사용하고 있다. IPMAC 모델의 운영체제는 Widow 2000 Pro 이며 IPMAC 가 사용할 데이터베이스는 Oralce 데이터베이스이다.

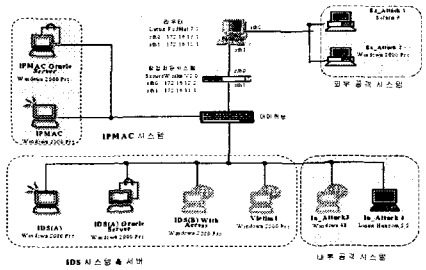

그림 7 실제 구축된 IPMAC 시스템 환경

5. 향후 연구 과제 및 결론

본 논문에서는 이기종 침입탐지시스템 운용 환경에서 침입탐지패턴 통합 및 대응을 위한 요구사항을 도출하고 통합 및 대응을 위한 IPMAC 모델 및 탐지알고리즘을 제시하여 관련 모듈을 설계 및 구현한 결과를 제안하였다. 본 논문은 이기종 네트워크 IDS 기반 IDS 를 중점을 두었으므로, 호스트 IDS 기반인 경우, IPMAC 를 구축하는 문제는 본 논문의 범위에 포함되지 않으며, 호스트 기반 IDS 에 적합한 패턴을 수집하는 기술에 대한 별도의 연구가 필요하다. 향후 침입탐지패턴을 그룹화하고 분류하는 기준 및 공격 유형을 최적으로 그룹화하고 분류하는 연구를 수행하여 IPMAC 에 맞는 실제 공격에 대한 공격 유형 분류가 필요할 것이다.

참고문헌

[1] John McHugh et al "The Role of Intrusion Detection Systems", IEEE SOFTWARE, 2000

[2] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion-Detection Alerts", RAID 2001, 2001.

[3] Magnus Almgren and Ulf Lindqvist "Application-Integrated Data Collection for Security Monitoring", RAID 2001

[4] Eugene Spafford and Diego Zamboni, "Data collection mechanisms for intrusion detection system", RAID 2001, 2001

[5] Peng Ning et al, "Analysing Intensive Intrusion Alerts via Correlation", RAID 2002, 20002.

[6] A Mission-Impact-Based Approach to INFOSEC Alarm Correlation, RAID 2002, 20002.

[7] 한국정보보호진흥원, "침입탐지시스템 평가기준 해설서", 2001

[8] D. Denning, " An Intrusion Detection Model," IEEE Transactions on Software Engineering, 13(2), February 1997

[9] K. Tan, K. Killourhy, and R. Maxion, 괿 ndermining an Anomaly-Based Intrusion Detection System using Common Exploits, *RAID 2002*, Zurich, Switzerland, October 2002

[10] S. Axelsson, Intrusion Detection Systems: A Survey and Taxonomy, *Technical Report 99-15*, Chalmers University, March 2000