침입탐지 시스템 관리를 위한 침입경보 축약기법 적용에 관한 연구*

김석훈** · 정진영*** · 송정길****

요 약

네트워크 시스템에 대한 악의적인 접근과 정보위협이 증가하고, 그 피해또한 기업에서 개인 사용자까지 확대되고 있다. 침입탐지 시스템, 침입차단 시스템 등 단위 보안 기능만을 제공하는 제품은 분산화, 지능화 되어가고 있는 복합적인 침입에 대한 대응에 한계가 있다. 여러 보안 제품을 연동하여 해커의 침입탐지, 대응 및 역 추적을 위한 통합 보안 관리의 필요성이 대두되고 있다. 그러나 통합보안 관리의 특성상 다양한 보안 제품에서 전송된 이벤트와 침입경보의 양이 많아 분석이 어려워 서버측의 부담이 되고 있다. 따라서 본 논문에서는 이러한 문제점을 해결하고자 침입경보 데이터를 축약하는 방법에 대하여 연구하고자 한다.

A Study on Intrusion Alert Redustion Method for IDS Management*

Seok-Hun Kim** · Jin-Young Jeong*** · Jung-Gil Song****

ABSTRACT

Today the malicious approach and information threat against a network system increase and, the demage about this spread to persnal user from company. The product which provides only unit security function like an infiltration detection system and an infiltration interception system reached the limits about the composition infiltration which is being turn out dispersion anger and intelligence anger. Necessity of integrated security civil official is raising its head using various security product about infiltration detection, confrontation and reverse tracking of hacker. Because of the quantity to be many analysis of the event which is transmitted from the various security product and infiltration alarm, analysis is difficult. So server is becoming the charge of their side. Consequently the dissertation will research the method to axis infiltration alarm data to solve like this problem.

Key words : IDS, IDMEF, Intrusion, Alert Redustion, ESM

---

* 본 연구는 '산업자원부 지역협력연구사업(과제번호 : R12-2003-004-02001-0) 지원으로 수행되었음'.

** 한남대학교 대학원 컴퓨터공학과 박사과정(교신저자)

*** 대전보건대학 멀티미디어과 조교수

**** 한남대학교 정보통신 · 멀티미디어공학부 교수

1. 서 론

정보통신 주요 기반 시설에 대한 분산화가 되고 지능화되는 침해행위 및 위협이 급속도로 증가하고 있고, 장비 위주의 네트워크 인프라는 관리의 분산, 통합의 어려움, 트래픽 보장의 어려움, 보안과 인증의 분산 등 여러 가지 문제를 가지고 있다. 특히, 불법적인 침입이 다양해짐에 따라 각각의 통제가 어려우며, 갈수록 다변화 된 침입에 대하여 대처하기가 어렵고, 시스템 환경에 적합한 시스템 개발과 대규모 네트워크에 대한 효율적으로 대응할 수 있는 통합 보안 관리의 필요성이 대두되고 있다[1, 2].

통합 보안 관리 제품들은 초창기에 단순한 이벤트를 직접 받아 모니터링에서 검색엔진을 추가하여 보안관리자로 하여금 보안 로그를 손쉽게 확인 할 수 있도록 기능이 확장되었다. 특히, 인가받지 않은 외부 침입자를 실시간으로 탐지하여 침입에 대한 즉각적인 대응, 역 추적까지 할 수 있는 보안 통합 개념의 관제 서비스로 발전되고 있다. 그러나 다양한 보안 제품을 활용하기 때문에 전송되는 이벤트 및 침입 경보의 양이 많아 분석이 어렵고 서버의 부담이 되고 있다. 침입탐지 시스템의 문제점중 대표적인 부분이 과탐지로 인한 경보메세지 과다 및 경보메세지 중복, 많은 양의 경보메시지에 의한 관리의 어려움이다. 이로 인하여 보안관리자의 업무가 증가하게 되어 침입에 대한 적절한 대응을 하지 못하거나 또는 보안인력을 추가로 필요로 하게 되었다[3]. 따라서 본 논문에서는 침입탐지시스템에서 경보메세지를 축약하는 구조를 분석하여 프로토타입 시스템을 제안하고자 한다. 침입 경보 축약기법을 적용해 중복 매시지가 발생하지 않도록 설계하였다.

본 논문의 구성은 2장에서는 침입탐지 시스템에 대하여 기술한 후 경보메세지 축약방법을 살펴본 후 3장에서는 데이터 축약을 위한 효율적인 시스템을 제안하였고 4장에서 침입탐지 프로토타입 시스템을 구현하고, 결론 및 향후 연구방향을 제시한다.

2. 관련 연구

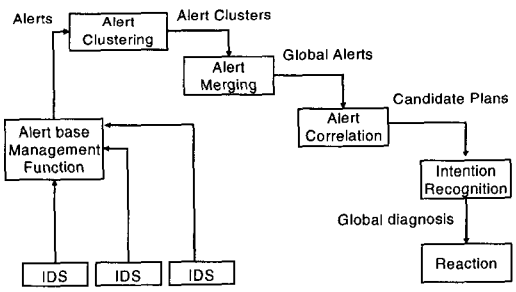
2.1 침입탐지 시스템

IDS는 Intrusion Detection System(침입탐지시스템)의 약자로, 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행 중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다. 침입이란 시스템에 대한 고의적 불법적인 행위를 말하며 시스템의 불법침입, 중요정보의 유출 및 변경, 훼손, 불법적인 사용, 그리고 컴퓨터 바이러스 및 서비스거부 등과 같은 구체적인 형태로 나타난다. 침입탐지시스템은 이러한 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그파일분석에서부터 복잡한 실시간 침입탐지시스템까지 다양한 소프트웨어가 존재한다. 침입탐지 기법은 크게 비정상적인 침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다.침입탐지 시스템은 오늘날의 복잡해지는 대규모 네트워크 환경에 있어서 매우 큰 비중을 차지한다. 고전적인 침입 탐지 시스템은 침입자의 새로운 행동 패턴 또는 변형된 행동 패턴의 침입을 탐지하거나 대응이 불가능 하고 수동적이며, 사후 조치라는 취약성으로 인하여 실제적인 정보보호에 도움을 주지 못하는 실정이기 때문에, 현재 실정에 부합하는 자동화된 침입 탐지 시스템이 네트워크 환경에서 요구된다. 기존의 제품화된 시스템들은 각각의 특징을 가지고 있지만 사후 감사 추적의 특징

으로 인해 즉각적인 대응 조치가 미약하고, 실시간 패킷 분석의 부분적인 침입 탐지는 아직 전체적이고 포괄적이며 자동적인 침입탐지 기술을 필요로 하는 현재의 네트워크 컴퓨팅 환경에는 매우 취약한 맹점을 가지고 있다.

2.2 CRIM

CRIM은 MIRADOR 프로젝트 내에서 개발된 침입탐지시스템간의 협동 모듈이다. 프랑스 국방연구소는 협동적이고 적응적인 침입탐지시스템 플랫폼을 개발하기 위해서 MIRADOR 프로젝트를 시작했다. CRIM은 그림과 같이 다섯 개의 함수로 구성되어 있다[6, 7].

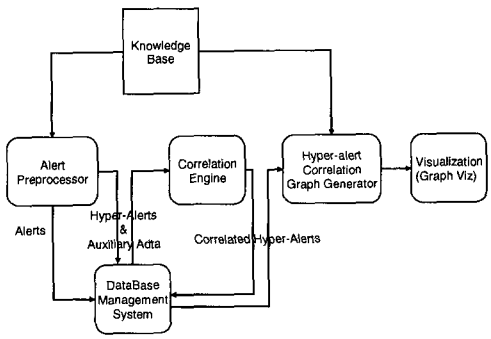


(그림 1) CRIM 구조

- 침입경보베이스 관리함수 : 여러 침입탐지시스템에서 생성된 침입경보를 IDMEF 형태로 받아 관계형 데이터베이스에 저장한다.
- 침입경보 군집화함수 : 데이터베이스에 접근하여 침입경보의 군집을 생성하고, 동일한 공격에 해당하는 침입경보를 인지하고자 시도하고 침입경보들을 유사도에 따라 군집에 포함시킨다.
- 침입경보 통합함수 : 각 군집을 대표하는 침입경보를 생성하거나 갱신한다.
- 침입경보 연관관계함수 : 보안 관리자에게 보다 통합적인 정보를 제공하기 위해 침입경보 통합함수에 의해 성성된 군집 침입경보를 분석하고 연관시킨다.
- 공격의도 인지함수 : 공격계획의 집합에서 공격계획을 하나씩 대입하여 실제 공격을 파악한다.

2.3 Hyper-alert Correlation Graph

노스캐롤라이나 주립대학의 Peng Ning은 침입경보 연관관계의 시각적 분석이 가능한 Hyper-alert Correlation Graph를 제안하였다. (그림 2)는 Peng Ning이 제안한 Intrusion Alert Correlator의 구조를 보여주고 있다.



(그림 2) Intrusion Alert Correlator 구조

침입경보 연관관계 분석기는 지식베이스, 침입경보 전처리기, 연관관계 분석엔진, Hyper-alert Correlation Graph 생성기, 시각 컴포넌트로 구성되어 있다. 시각 컴포넌트를 제외한 다른 컴포넌트들은 모두 데이터베이스와 상호 작용한다.

2.4 경보메시지 축약 기법

경보메시지 축약을 위한 기존 연구는 대표적으로 확률적인 방법, ACC 및 선행조건 방법이 있다. 확률적인 방법은 경보메시지의 유사성을 평가하여 한계값을 초과하는 경우 이들을 하나로 통합

한다. 침입탐지에 의해 생성된 경보메시지를 사용하지 않고 표준화된 기준에 따라 재분류하고 이를 확률적인 방법으로 통합한다. 통합방법으로 새로운 경보메시지가 발생시 이전에 발생한 경보메시지들과 유사성을 평가하여 가장 근접되게 일치하는 그룹과 통합하고, 일치하는 경보메시지가 없을 경우 새로운 그룹을 생성한다.

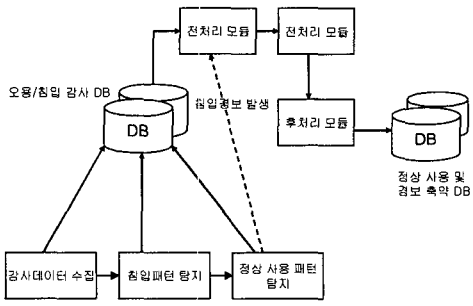
ACC방법은 경보메시지가 동일성을 가지거나 순서를 가지는 경우(correlation)와 상황별 유사성을 가지는 경우(aggregation)로 나누어 통합을 수행한다. 시스템 구성을 그림과 같이 계층화된 분산구조를 지원하며 표준화되지 않은 경보메시지 형식을 사용하는 침입탐지 시스템들을 위해서 Pre-adapter를 사용하여 IDMEF로 변환한다. 이 방법은 미리 정의된 상황에 들지 않는 유사한 경보 메시지들에 대해서 그룹화를 하지 못하고 순서가 고정되어 있고 연관된 모든 경보메시지들에 대한 통합을 제공하기 위한 정보가 충분하지 않다.

선행조건 방법은 경보메시지가 발생시 선행조건을 이용하여 그것을 만족하는 경우 경보메시지를 통합한다. 하나의 공격이 성공하기 위해서는 선행되어 실행되어야 할 공격들과 공격이 성공했을 경우 예상되는 결과나 이어질 공격들을 수식으로 계산하여 경보메시지를 통합한다. 하나의 공격이 성공하기 위해서는 선행되어 실행되어야 할 공격들과 공격이 성공했을 경우 예상되는 결과나 이어질 공격들을 수식으로 계산하여 경보메시지 통합을 수행한다. 이 방법은 연산에 많은 시간이 소모되어 실시간으로는 부적절하고 선행조건이 없는 경우 통합을 수행하기 어렵다.

3. 시스템 설계

3.1 시스템 구성

본 논문에서 제안한 침입경보 축약 IDS 시스템은 침입경보 수집기, 침입경보 전처리기, 침입경보 후처리기로 구성되어 있다. 침입경보 수집기는 침입탐지시스템으로부터 필터링 과정을 거쳐 전송된 침입경보를 받아 침입경보 데이터베이스에 저장한다. 침입경보 전처리기는 일반적인 통합보안관리 모델에서 각 HOST에서 보내어지는 감사데이터, 침입패턴, 침입경보를 보낼때 불필요한 침입경보들을 줄여서 보내줌으로서 침입경보 분석의 효율성과 네트워크 트래픽을 줄일 수 있다.



(그림 3) 침입경보 IDS 구성

3.2 침입 탐지 시스템 패턴 알고리즘

다음 알고리즘에서와 같이 A2는 새로운 침입 패턴과 정상 데이터로부터 학습된 추가된 분류자이며 알고리즘에서 결정 규칙은 출력을 위해서 평가된다.

```
Intrusion_alert()
{
 if (A1(x)=normal) || (A1(x)=anomaly) then
  // 정상패턴과 비정상 패턴 분류
 if A2(x) = normal
    then output ← A1(x)(normal or anomaly)
  // 존재하는 침입 패턴 모델
    else output ← new_intrusion
    else output ← A1(x)
}
```

A1은 존재하는 침입 탐지 시스템 모델이고 A2는 새로운 침입 패턴을 위해 훈련된 새로운 모델이다. A1에서는 정상과 비정상 패턴만을 확인하고

새로운 침입을 확인할 수 없기 때문에 대부분의 패턴들은 비정상과 오용으로 분류한다. 그러나 A2는 새로운 침입과 정상 데이터로 분류한다. 이때 새로운 침입 패턴의 양이 적기 때문에 A2는 다른 데이터로부터 침입 패턴을 쉽게 분류할 수 있다.

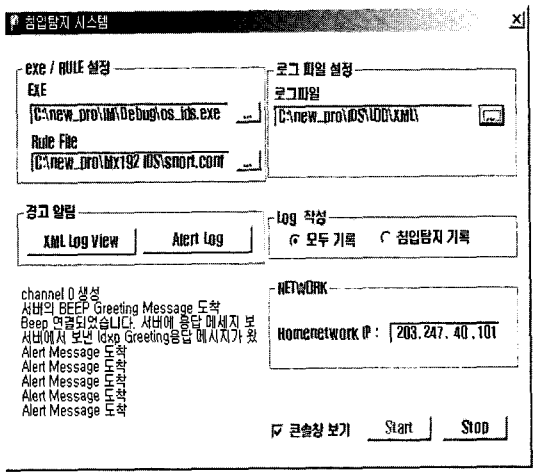
3.3 침입 탐지 시스템 모듈 설계

Rule pattern match와 Plug In 기반의 IDS는 각각의 Module을 가리킬 수 있는 Function pointer로 구성된 Linked list로 이루어져 있다. 따라서 새로 추가하고자 하는 부분은 그 List에 추가적으로 계속 덧붙일 수 있도록 구성되어 있다.

```
int OpenPcap()
 {
   bpf_u_int32 SubNet, NetMask;
   char error[PCAP_ERRBUF_SIZE];
   struct bpf_program fcode;
   if (g_progArg.szDevicename != NULL)
    {
If((g_fp=pcap_open_live(g_progArg.szDevicename,1514,1,20,
error))  == NULL )
    {
      fprintf(stderr, "\n어댑터를 오픈할 수 없습니다.\n");
      return -1;  }}
    else
     Usage();
   if(g_progArg.szFilterOption != NULL)
    {
   if(pcap_lookupnet(g_progArg.szDevicename,&SubNet,
&NetMask,
    error)<0)
      {
      fprintf(stderr,"\n넷마스크를 가져올 수 없습니다.\n");
        return -1;
        }
    if( g_progArg.nFilterOptionFlag )
     {
   if(pcap_compile(g_fp,  &fcode,  g_progArg.szFilterOption,
1,
    NetMask)<0)
     {
     fprintf(stderr,"\nError compiling filter:wrong syntax.\n
");
      return -1;
    }
```

4. 프로토타입 시스템 구현

(그림 4)는 초기 IDS를 설정할 수 있도록 구현한 부분으로서, 화면 상단에 있는 실행 File과 RuleSet의 경로가 나타나는데 이는 pcap을 설치하고 경로를 설정했을 시 프로그램 상에서 자동으로 알아서 설정되도록 되어있다. IDS가 생성한 침입경보를 표준화된 IDMEF 형태로 변환해 에이전트 시스템에 전달하고, 공격 유형에 따라 Alert 메시지들이 해당 경로로 자동 저장된다.



(그림 4) 침입탐지 프로토타입 시스템 구현 화면

5. 결론 및 향후 연구방향

침입탐지 시스템의 한계는 과탐지로 인한 경보메시지 과다 및 경보메시지 중복이 발생하여 침입판단 및 적절한 대응을 어렵게 한다는 것이다. 본 논문에서는 이러한 한계를 해결하기 위하여 침입경보 과다발생과 중복 메시지 발생에 대한 축약기법을 이용한 시스템을 제안하였다.

통합보안 관리 시스템에서 네트워크의 부하 및 시스템의 처리성능을 향상시키기 위하여 데이터 축

약이 중요한 역할을 하고 있지만, 이렇게 축약되어진 데이터를 가지고 관리자가 용이하게 어떠한 공격들이 발생하고 있는지를 파악할 수 있어야 한다.

향후 연구되어야 할 내용은 수집된 침입경보에 대한 연관성 분석을 통해 침입 탐지율을 향상방법과 취약성 분석 규칙을 이용한 방법, 관리자의 용이한 관리를 위한 침입 관리정책 적용에 대한 연구가 함께 이루어져야 할 것이다.

참 고 문 헌

[1] 한국정보 보호진흥원, http://www.kisa.or.kr

[2] 정보통신부, 해킹 바이러스 통계분석, 2004.

[3] 한국전자통신연구원, ESM 개발 동향, 2003. 5.

[4] IETF internet Draft, Intrusion Detection Exchange Format Data model, 2003.

[5] IETF internet Draft, Intrusion Detection Exchange Format Data Requirements, 2003.

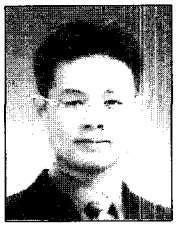
[6] N. Carey, A. Clark, and G. Mohay, "IDS Interoperability and Correlation Using IDMEF and Commodity Systems", ICICS 2002, LNCS 2513, pp. 252-264, 2004.

[7] 이성호 외, "침입경보 축약을 통한 규칙기반 연관관계분석기설계", 한국정보처리학회 춘계학술발표논문집, pp. 1091-1094, 2004. 5.

[8] 전상훈 외, "침입 복구 및 대응 시스템을 위한 실시간 파일 무결성 검사", 한국정보과학회 논문집, 제32권, 제6호, pp. 279-287.

[9] 송중석 외, "데이터 마이닝에 기반한 침입탐지 시스템의 탐지 정확도 향상에 관한 연구", 한국컴퓨터종합 학술대회논문집, pp. 208-210, 2005.

[10] 송정길, "이기종간 침입탐지 정보에 대한 웹기반 관리 시스템 설계", 한국사이버테러 정보전 학회논문집, 제5권, 제2호, pp. 65-74.



김 석 훈

2001년 배재대학교 정보통신 공학과(공학사)

2003년 한남대학교 대학원 컴퓨터공학과(공학석사)

2003년~현재 한남대학교 대학원 컴퓨터 공학과 박사과정 재학중

관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

정 진 영

1992년 한남대학교 전자계산학과 (공학사)

1994년 한남대학교 대학원 컴퓨터 공학과(공학석사)

2002년 한남대학교 대학원 컴퓨터공학과(공학박사)

2004년~현재 대전보건대학 멀티미디어과 조교수

관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

송 정 길

1966년 한남대학교 수학과 (이학사)

1982년 홍익대학교 대학원 전자계산학과(이학석사)

1988년 중앙대학교 대학원 전자계산학과(이학박사)

1990년~1991년 University of illinois 객원교수

관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산시스템, 정보보호