확장된 IDS 기능을 가진 IPS 설계에 관한 연구

나호준*, 최진호*, 김창수*, 박근덕**
*부경대학교 전자계산학과, **(주)센타비전

A Study on the Design of IPS with Expanded IDS Functions

Ho-Jun Na*, Jin-Ho Choi*, Chang-Soo Kim*, Gun-Duck Park**
*Dept. of Computer Science, PuKyong National University
E-mail : nahj@mail1.pknu.ac.kr, zonic1217@hanmail.net, cskim@pknu.ac.kr
**Centa Vision Crop.
E-mail : kdpark@centavision.co.kr

요약

최근의 침입탐지시스템(IDS: Intrusion Detection System) 기술동향은 Misuse 방식의 규칙 데이터베이스 변경에 대한 한계성 때문에 Anomaly 방식의 NIDS(Network IDS)에 대한 연구가 고려되고 있다. 현재 국내에서 개발된 기존의 제품들은 대부분 Misuse 방식을 채택하고 있으며, 향후 국제 경쟁력을 갖추기 위해서는 Anomaly 방식의 기술 연구가 필요하다.

본 연구에서는 본 연구실에서 개발한 NIDS를 기반으로 연관 마이닝을 이용한 비정상 탐지 문제, 내부 정보 유출 차단 등에 대한 통합된 시스템 설계 방향을 제시하여 국가기관이나 기업이 보다 안전하게 침입을 관리할 수 있는 IPS(Intrusion Prevention System) 시스템을 설계한다

1. 서론

본 논문은 본 연구실에서 개발한 침입탐지시스템을 근간으로 하여 통합된 IPS 시스템 설계 방향을 제시한다. 이러한 관점에서 현재 국내외 IDS 연구 동향을 알아본다.

국외 동향으로는 컴퓨터보안연구소의 주관으로 샌프란시스코 미연방수사국 컴퓨터범죄수사단과 함께 1996년 이후 매년 컴퓨터 범죄 및 정보보안 실태에 관한 설문조사를 실시해왔으며 작년에 6번째인 설문조사 결과에 따르면 보안기술별 사용현황은 아래와 같다. 응답자의 95%가 방화벽, 61% IDS, 90% 접근통제, 42% 디지털ID 등 다양한 보안기술을 사용하고 있는 것으로 나타났다. 2001년 조사에서 두드러지는 특징은 응답자 중 IDS 사용자수는 2000년 50%, 2001년 61%로 점차 증가하고 있으며, 이는 외부로부터의 시스템 침해를 탐지하거나 인터넷 접속으로 인한 피해 증가를 지적한 응답자가 계속 늘어나고 있는 점과 큰 연관이 있다. IDS가 이러한 침해상황을 탐지, 분석하도록 함으로써 각 기관들이 적극적으로 IDS를 도입하는 것으로 보고되고 있다[6].

국내 연구 동향으로는 인터넷 관련 정보산업이 꾸준히 성장세를 보이고 있고 특히, IDS 분야의 DRM과 비정상적 공격탐지 기능은 차세대 정보보호분야의 중요한 기술로서 자리 매김 할 것이 확실하기 때문에 매우 중요하다.

2. 기존 방화벽 및 IDS 기능 분석

1) 침입차단 시스템

다중 홈 게이트웨이(Multi-homed Gateway)방식이 주류를 이루고 있는 침입차단(Firewall) 시스템에서 패킷 필터링과 응용 게이트웨이를 이용한 접근제어가 주종을 이루고 있어 실시간 서비스거부 공격(DoS 혹은 DDoS)에 대해 능동적인 대응이 불가능하다. 그리고 관리자에 의한 수동적인 보안 정책 및 보안 규칙 설정에 의해 운영하게 되어 매우 비효율적이고 수동적인 한계에서 벗어나지 못하고 있다. 이것은 보안 관

리자로 하여금 끝없는 운영관리 노력과 정보 수집에 많은 시간을 소비하게 하는 요인으로 작용하고 있다. 또한, 침입차단시스템에서 제공하는 침입탐지기능은 대부분 해킹의 시작 단계인 정보 수집에 관련된 몇 가지 공격 패턴에 한정되어 있고, 실시간 업데이트가 되지 않아 다양한 침입 및 공격에 대응하기에 역부족이다. 그리고 정보수집 공격 탐지 및 방어는 침입탐지시스템 자기 자신을 보호하는 목적으로 사용하는데 한정되어 있다.

침입차단시스템의 처리속도 및 성능 저하를 고려하여 수집된 패킷의 헤더와 일부 데이터만을 가지고 접근제어를 수행하다 보니 손쉬운 서비스거부공격 조차도 탐지할 수 없을 뿐 아니라 근본적인 차단시스템의 방어 역할을 수행하지 못하고 있다. 침입탐지시스템을 경유한 패킷에 대해 접근제어를 수행한 감사기록이 관리/보존하고는 있지만, 그 기록에 관한 분석이 시스템 상에서 전혀 이루어지지 않고 있다. 이것은 비슷한 유형의 침입 혹은 공격에 대해서도 대응할 수 있는 기본 데이터를 관리자에게 제공하지 않을 뿐 아니라 차단시스템 자신도 알지 못한다. 감사기록을 생성하는 시스템 노력에 비하면 그 쓰임새가 매우 단순한 것이다. 아울러 새로 발견되는 신종 침입/공격 유형에 대해서는 말할 것도 없이 적절한 대응 방법이 없는 것이다.

기존의 침입차단시스템과 침입탐지시스템의 기능을 단순히 결합하는 형태의 결합형 보안시스템은 전체적인 처리 성능 저하를 유발할 가능성이 높고, 시스템 자원을 필요이상 소비하여 더욱 향상된 시스템 하드웨어 환경을 요구하게 되어 경제적이지 못하고, 신종 혹은 변종 침입/공격 유형에 역시 대처할 수 없는 비지능형이기에 지양해야만 한다.

2) 침입탐지시스템

현재의 네트워크 기반 IDS는 Passive 방식을 대부분 채택하고 있어 자신으로 인한 네트워크 성능 저하를 유발시키지 않는데 급급하여 탐지 및 방어수준이 기본적이다. 실례로 TCP 기반의 공격 및 침입 유형에 대해서는 세션 리셋(Reset)을 이용하여 대응할 수 있으나 UDP, IP 기반의 공격 및 침입 유형에는 대응할 수 없다. 이것은 Passive 방식의 침입탐지시스템이 가지고 있는 매우 취약한 점이 아닐 수 없다. 그래서 대부분의 Passive 방식의 침입탐지시스템은 이런 취약점을 극복하고자 다양한 침입차단시스템과 연동을 꾀하고 있고, 실제로 이것은 시스템 관리자나 각 보안 제품의 기능발휘에 오버헤드로 작용하고 있다. 또한 둘 중의 한 시스템이라도 down이 된다면 보안에 매우 취약한 상황이 초래되는 것이다. Passive 방식의 침입탐지시스템은 Low-level의 패킷필터링 조차도 할 수 없기 때문에 그 기능을 침입차단시스템에게 의존하고 있는 것이다. 놀라운 것은 Passive 방식의 침입탐지시스템은 스스로 방어할 수 있는 방법이 없기 때문에 내/외부로부터의 공격에 매우 취약하다. 자신을 은폐할 수 있는 기능을 탑재하고 있기는 하지만 침입탐지시스템 구조상 우회경로가 존재하기 때문에 은폐기능이 공격에 대한 근본적인 방어 수단이 될 수는 없다.

오남용(Misuse) 기법만을 대부분 이용하는 기존의 침입탐지시스템은 매우 개발사에 의존적이고, 수동적인 시스템일 수밖에 없다. 변종 혹은 신종 공격/침입 유형이 발견된 경우 개발사에서 자사 침입탐지시스템에서 사용하고 있는 규칙 데이터베이스를 갱신(Update)해 주지 않는다면 방어가 전혀 불가능하다. 또, 개발사가 파산한 경우 해당 침입탐지시스템을 사용하고 있는 고객의 입장에서는 규칙 데이터베이스 갱신이 잘되는 다른 제품을 구입해야하는 경제적인 부담이 발생하는 것이다. 오남용 기법만을 사용하는 침입탐지시스템의 경우 외부의 공격 혹은 시스템 장애로 인한 규칙 데이터베이스를 도난 혹은 파괴당했을 경우 탐지시스템으로의 역할을 전혀 수행할 수 없다. 즉 규칙 데이터베이스는 침입탐지시스템에게 매우 중요한 자원으로 마땅히 보호되어야 함에도 불구하고 관리에 매우 허술하다. 결론적으로 기존의 침입탐지시스템은 매우 수동적이며 방어 능력이 허술할 뿐 아니라 자기 자신을 보호함에 있어서도 매우 취약하다.

3. 확장된 IPS 설계

1) 기존 NIDS의 확장된 IPS 설계

아래 [표 1]은 기존에 개발된 NIDS를 기반으로 확장된 IPS를 위한 주요 기능을 기존 네트워크 기반 IDS(NIDS)의 기능과 표로 나타낸 것이다. 본 연구에서 확장된 IPS 기능으로 추가하고자 하는 것은 기존의 방화벽 기능은 물론 IDS가지고 있는 기능과 비정상탐지 기능, DRM을 이용한 내부문서 유출 방지 기능 등을 통합적으로 운영할 수 있는 시스템을 설계하는데 있다. 이를 위해 본 연구에서 개발하는 주요 내용은 [표 1]에서 나타낸 바와 같이 탐지모델과 내부문서 파일 유출 대응기술, 비정상탐지를 위

한 연관마이닝 기법의 새로운 접근 방법, 침입자 관리 및 역추적을 수행할 수 있는 Honey Pot 개념의 관리 기법 등이 포함된다. 이러한 내용들은 기존의 IDS에서 일반적으로 포함하고 있지 않는 기능으로 본 논문에서는 기존의 IDS 기능에 부분적으로 이러한 기술들을 추가한 새로운 접근 방법의 확장된 IPS(Intrusion Prevention System)을 설계한다([표 1] 참조).

[표 1] 확장된 IPS의 주요 기능들

NO	주요기술	기존 NIDS	확장된 IPS
1	탐지모델	Misuse	Misuse+ Anomaly
	대응기법	Passive	Active
2	Predictive Anomaly 탐지 기술	-	연관마이닝 기법
3	Active 대응 기술	Only TCP	Packet Filter, TCP Reset
4	감시기능강화 기술 (관리기능강화)	-	Virtual Honey Pot
5	신종/변종 패턴 탐지	-	Yes
6	파일유출 대응기술 (저작권/소유권 보호)	-	DRM 기법
7	무결성 체크	Yes	Yes
8	감사기록	Yes	Yes
9	보고서(통계)	Yes	Yes
10	실시간 경보	Yes	Yes
11	원격관리	Yes	Yes
12	암호화 (원격관리)	SSL/SEED	SSL
13	규칙 DB 자동 갱신	Yes	Yes
14	Giga Ethernet 지원	Yes	Yes
15	자체 DB 암호화	Yes	Yes

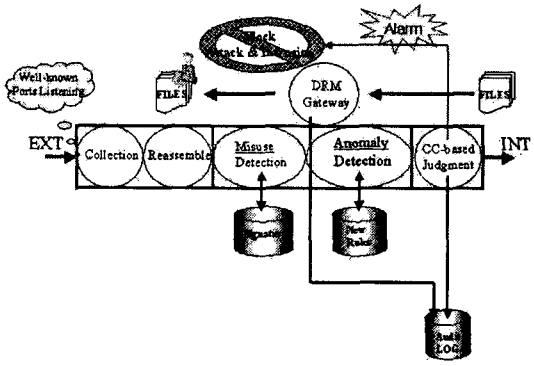
2) IPS의 전체적인 구성도

본 연구실에서는 K4 등급에 기초한 IDS를 개발하였다. 이러한 기능은 [표 1]의 기존 NIDS에서 제시하는 기능들이 포함되어 있다. 이러한 기능들에 새로운 접근 방향으로 확장된 NIDS를 설계하기 위해 [그림 1]과 같은 구성안을 제시하며, 아래 기술한 내용들은 전체적인 구성에 대한 세부 설명이다.

① 비정상 공격 탐지기능

인터넷 환경에서 네트워크 기반의 불법 침입 유형들에 대해 이미 알려진 침입 정보를 이용하여 변형된 불법 침입의 탐지를 위한 침입시나리오 자동 탐지 알고리즘이 필요하다. 이를 위해 본 연구에서는 기존의 상태전이 기법과 연관 마이닝 알고리즘을 활용하여 비정상(anomaly) 탐지가 가능한 방법을 찾을 수 있는 방향으로 설계안을 제시한다.

[그림 1] 확장된 IPS의 전체적인 구성도

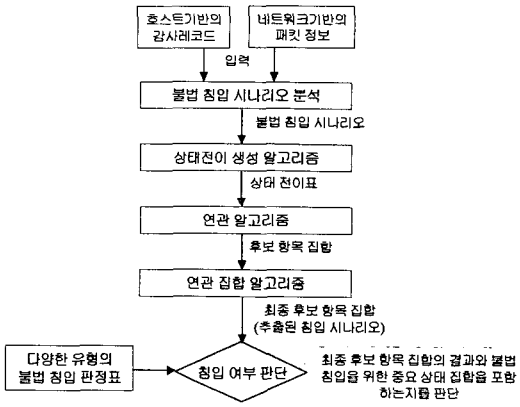


연관(associate) 알고리즘은 기본적으로 다음과 같이 수행된다([그림 2] 참조).

ⓐ 단계 1: 호스트기반의 감사레코드와 네트워크 기반의 패킷 정보를 입력으로 받아서 불법침입 시나리오 분석 기법에 의해 침입으로 예측되는 상태정보를 저장한다.

ⓑ 단계 2 : 저장된 상태 정보들을 이용하여 일반적으로 많이 알려진 상태전이 기법으로 상태전이표를 생성한다. 이와 같이 생성된 상태전이표는 불법 침입과 관련된 정보들을 검색하기 위한 기초 자료로 활용한다.

[그림 2] 연관마이닝에 의한 비정상 탐지



ⓒ 단계 3 : 연관 알고리즘은 상태전이표에 저장된

데이터를 기준으로 각 상태에서 발생한 정보들의 연관성을 찾기 위해 후보항목집합을 생성한다. 생성된 후보 항목집합은 항목들의 연관성을 기반으로 축약된 최종후보 항목집합을 생성하게 된다. 이와 같은 최종 후보항목 집합의 결정은 비정상탐지를 위한 중요한 임계값으로 결정된다.

ⓓ 단계 4 : 기존의 침입 유형에 의한 불법침입 판정표를 기반으로 최종 후보 항목집합의 속성을 비교하여 사전에 입력한 임계값의 범위를 넘어서면 비정상 불법 침입으로 판정하여 관리자에게 정보를 알려주는 기능을 한다. 최종적인 불법 침입은 관리자가 네트워크 세션 접속에서부터 입력된 log 정보를 분석하여 불법 침입 여부를 결정하게 된다.

② 내부 문서유출 관리 기능

기존의 IDS의 경우 외부에서 내부로 들어온 불법 침입에 대해 침입을 탐지하지만 최근에는 내부 문서 유출에 대한 탐지 기능을 추가하고 있다. 본 연구에서는 대부분의 기존 IDS에서 제공하지 않는 내부 문서 유출 탐지 기능을 추가하기 위해 다음과 같은 방법으로 설계안을 제시한다.

ⓐ 파일의 중요도에 따른 권한 부여 방법

㉠ 모든 내부사용자 전송가능 = nobody

㉡ 관리자급이 아닌 사용자 = normal

㉢ 관리자급 사용자 = root

파일이 전송될 때 전용 게이트웨이에서 사용자의 권한을 검사하여 권한을 벗어나는 전송에 대해서는 IPS가 제어할 수 있는 기능을 추가한다. 본 설계안은 사용자별로 부여된 사용자 ID와 패스워드의 인증 이후에 전송 게이트웨이의 사용이 허가된다.

ⓑ 파일이 전송될 때 워터마킹된 자료 전송

파일의 헤더 포멧에 워터마킹의 유무 필드를 넣어 워터마킹된 파일에 한해 전송된다. 그리고 워터마킹 삽입 패턴으로는 유닉스 사용자 ID를 키값으로 삽입한다.

ⓒ 게이트웨이에서의 검사 기능

전용 게이트웨이를 통해서만 파일이 전송되어 게이트웨이에서 검사하는 리스트는 사용자의 권한, 워터마킹 유무 등이 포함되며, 정보 전송은 인증 후 전송되므로 투명성을 보장받을 수 있으며, 불법적인 전송에 따른 확인이 가능하다.

ⓓ 로그 처리

전용 게이트웨이를 통하여 전송된 파일은 파일이름, 사용자, 시간 등의 로그를 남기도록 설계하였다.

4. 결 론

본 연구에서는 기존에 본 연구실에서 개발한 네트워크 기반 침입탐지시스템[7]의 기능을 확장한 침입방지시스템(IPS) 설계를 위한 구성도를 제안하였다. 제안한 IPS 기능은 기존 IDS 기능에서 연관마이닝 기법을 적용한 비정상 탐지기능과 내부문서 유출기능이 추가된 문서유출 탐지기능이 포함되어 있다.

현재 본 연구에서는 앞에서 제시한 전체적인 구성도를 기반으로 내부 알고리즘을 설계하고 있으며, 일부 모듈에 대해서는 구현 작업을 진행하고 있다. 또한 기존의 방법은 응용 계층의 libpcap을 이용한 패킷 캡쳐를 수행하고 있었으나 현재는 네트워크 계층에서 패킷을 수집하는 모듈을 구현하고 있다.

[참고문헌]

[1] 한국전산원, "유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구", NCA VI-RER-95105, 1995. 12.

[2] 한국정보보호센터, "침입 탐지 모델 분석 및 설계", 1996. 9.

[3] 변경근, 심영철, 신훈, 임휘성, 임채호, "전산망보안점검도구의 설계 및 구현", 한국통신정보보호학회 종합학술발표회 논문집 Vol.6 No.1, 1997. 6.

[4] 포항공과대학 전자계산소, Security Plus for UNIX, 1998. 3.

[5] 양동수, 외 4명, "네트워크 기반의 침입탐지 시스템 및 관리 모듈 설계 및 구현", 한국해양정보통신학회 춘계학술대회발표집, Vol. 5, No. 1, pp. 680-683. 2001. 5.

[6] 황성원, "2001년 CSI/FBI 컴퓨터 범죄 및 보안서베이 결과분석",KISA 정보보호정책 동향 분석, 2001. 6.

[7] 김창수, "네트워크 기반의 침입탐지시스템", 부경대학교 SSMCL 연구보고서, pp. 1- 400, 2002. 1.

[8] D.B. Chapman, "Network (In)Security Through I.P Packet Filtering", Sep, 1992.

[9] Atkins, Buis, Hare, Nachenberg, Kelley, Nelson, Phillips, Ritchey, Steen, "Internet Security", New Riders Publishing, 1996.

[10] T. H. Ptacek and T. N. Newsham, "Insertion, evasion, and denial of service: Eluding network intrusion detection.", Technical report, Secure Networks, Inc., Jan 1998.

[11] http://www.inzen.com

[12] http://www.penta.co.kr