내장 IDS기반의 통합 보안관리 시스템 개발

허승표*, 전예환*, 김점구*
*남서울대학교 컴퓨터학과
email:huhspunk@gmail.com

Development of Integrated Security Management Based on Cloaking IDS

Seung-Pyo Huh*, Ye-Hwan Jeon*, Jeom-Goo Kim*
*Dept of Computer Science Namseoul University.

요 약

본 연구에서는 서비스를 제공하는 각 서버들을 위협에서 보호하고 통합적으로 관리하기 위해 내장 IDS기반의 통합 보안관리 시스템을 개발하였다. IDS 서버를 외부망과 단절시킴으로써 IDS 서버에 대한 위협 자체를 원천적으로 차단하였고, 관리 대상 서버들에 에이전트를 탑재하여 탑재된 에이전트가 서버의 시스템 자원 및 네트워크 트래픽, 위협이 되는 패킷들의 자세한 정보를 수집, 분석하여 관리서버로 전송한다. 관리 프로그램은 비동기식의 X-Internet기술을 도입한 Adobe Flex를 사용한 웹 어플리케이션으로 개발하여 어떤 플랫폼에서도 접속하여 관리자의 역할을 수행할 수 있도록 하였다. 이와 같은 관리 프로그램을 통하여 대상 서버들의 시스템 자원 및 네트워크 트래픽들을 효율적으로 파악할 수 있고 IDS에서 탐지한 위협을 탐지 및 차단이 가능하도록 구현하였다.

1. 서론

최근 매스컴 보도에 의하면 현재 600만개의 해킹 기법이 존재하며, 매년 몇 백만개씩이 새롭게 만들어지고 있다고 한다. 이에 따른 보안 침해는 국가적인 문제를 떠나 국제적인 문제이며, 경제적인 피해는 심각한 규모로 늘어가고 있다. 그럼에도 정보시스템들은 조직의 핵심 업무처리를 담당하고 있을 뿐만 아니라 경쟁 우위 확보를 가능하게 하는 전략적 도구로서 자리를 굳혀 가고 있다.

공공기관이나 기업은 이러한 정보시스템에 대한 접근제어, 무결성, 그리고 가용성 등 보안성 유지를 위해 노력하고 있지만 새로운 침해기술 등장, 그리고 관리상의 문제점 등 시스템의 성능이 저하되거나 장애가 발생하게 되어 적절한 업무 처리가 불가능하게 되고 경우에 따라 상당한 금전적 손실을 가져오게 되는 경우가 자주 발생하고 있다. 이러한 문제점을 해결하기 위한 방법으로 우선 정보시스템들을 통합적으로 관리하는 방법이 절실히 요구되고 있다.

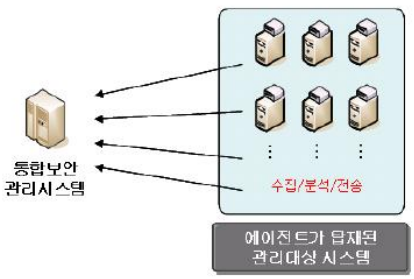
본 논문은 활용성과 효율성, 안전성을 강조한 에이전트를 이용한 내장 IDS기반의 통합 보안관리 시스템을 제안하고 개발하였으며, 이 시스템으로 각 서버들을 효율적으로 관리할 수 있으리라 기대한다.

2. 관련 연구

2.1 시스템 자원 수집, 분석

웹 서버, FTP서버, 메일 서버 등은 각자 목적과 역할에 따라 서비스를 제공하고 있다. 통합 보안관리 시스템은 이런 서비스를 제공하는 정보시스템들이 아무런 무리 없이 잘 작동하고 있는지 어떤 이상 징후를 보이는지 등을 알기 위해 시스템 자원 현황과 네트워크 트래픽 등의 데이터를 실시간으로 관리 서버에 전송해야 한다.

데이터를 수집/분석하는 시스템을 별도로 두지 않고 관리 대상이 되는 각 서버에 에이전트를 탑재하여 탑재된 각각의 에이전트가 시스템 자원현황과 네트워크 트래픽 등의 정보를 수집/분석하여 관리 서버로 실시간으로 전송한다.



[그림1] 에이전트를 이용한 구성도

[그림1] 과 같이 관리 대상이 되는 각 서버에 에이전트를 탑재했을 경우 시스템의 리소스를 일부 사용하지만 수집/분석하는 시스템을 별도로 사용할 경우보다 오히려 데이터 전송을 위한 과다 네트워크 트래픽의 감소 및 자원

본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음

의 효율성이 극대화 된다.

CPU	시스템·유저·유휴 및 총 사용율
Memory	전체량, 사용량, 사용가능량
Disk	전체량, 사용량, 사용가능량
Swap	전체량, 사용량, 사용가능량
Network	수신패킷량, 송신패킷량

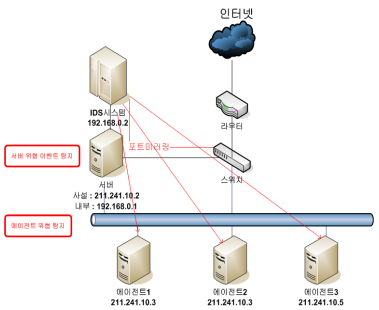
[표1] 에이전트가 수집/분석하는 데이터

[표1] 과 같은 데이터를 에이전트는 실시간으로 지속적으로 수집/분석하여 관리 서버에 전송하고 관리 서버는 각 에이전트에서 데이터를 전송받는 즉시 데이터베이스에 저장하게 된다.

2.2 내장 IDS 기반 침입탐지 및 분석

기존의 IDS 구축 사례를 보면 IDS가 서비스를 제공하는 해당 서버에 직접 구축되어 있거나 여러 호스트들을 탐지할 수 있는 형태로 구성되어 있다고 해도 외부망에 직접 노출이 되어 있는 형태이다. 전자의 경우는 각각 관리를 해야 하므로 통합 관리의 어려움이 있고 후자의 경우는 IDS서버가 위협을 받아서 제 기능을 상실할 우려가 있다.

이런 점들을 보완하기 위해 본 연구에서는 내장 IDS 기반의 침입탐지 시스템을 구축·개발하였다. 내장 IDS 기반 침입탐지 시스템은 서버와 모든 관리대상에 있는 에이전트들의 위협으로부터의 실시간 탐지 및 분석을 할 수 있다.



[그림2] 내장 IDS 기반 침입 탐지 시스템

[그림2] 와 같이 IDS시스템은 외부망과 단절되어 하나의 서버와 단일망으로 구성된다. 이렇게 구성된 IDS는 스위치의 기능인 포트 미러링을 사용하여 사설 IP를 부여하지 않아도 같은 스위치상에 있는 관리 대상이 되는 모든 서버들의 탐지된 위협 이벤트들을 수집할 수 있다. 또한 이렇게 구성된 IDS시스템은 외부에서 보이지가 않기 때문에 외부의 공격 이전에 탐지 자체가 불가능하게 된다.

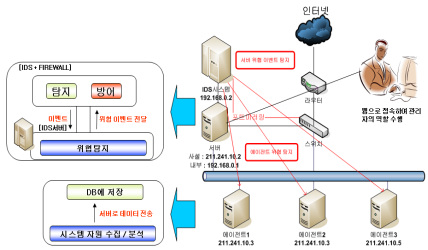
IDS시스템이 탐지한 각 에이전트들의 위협 이벤트는 실시간으로 분석하여 관리 서버의 데이터베이스에 저장된다. 위협 이벤트들의 위험도에 따라 분류하여 위험도가 높은 위협들에 대해서는 능동적인 대처가 가능하도록 개발하였다.

3. 내장 IDS기반의 통합 보안관리 시스템 설계

IDS서버가 외부에 탐지되지 않게 숨겨져 있는 내장 IDS기반의 통합 보안관리 시스템은 에이전트에서 지속적으로 시스템 자원 및 네트워크 트래픽을 수집/분석하여 관리 서버로 전송하여 이상의 유무를 파악할 수 있도록 하고 또한 IDS서버가 에이전트가 탑재된 관리대상 서버의 위협 이벤트를 실시간으로 분석하여 관리 서버에 전송함으로써 관리 서버는 종합적으로 시스템을 관리하고 분석하며 위협을 차단할 수 있게 설계하였다.

3.1 내부 시스템 구성

내장 IDS기반의 통합 보안관리 시스템은 데이터베이스를 포함하고 있는 관리 서버와 IDS서버,에이전트로 구성되어 있다.[그림3]



[그림3] 전체 구성도

에이전트는 해당하는 서버의 CPU, Memory, Disk, Swap, Network 데이터를 실시간으로 지속적으로 수집/분석하여 관리 서버에 전송하고 관리 서버는 각 에이전트에서 데이터를 전송받는 즉시 구축되어 있는 데이터베이스에 저장하게 된다.

위협의 원천적인 차단을 위해 외부망과 단절되어 오직 관리 서버와 1:1로 연결되어 있는 IDS서버는 스위치의 기능인 포트 미러링을 사용하여 사설 IP를 부여하지 않아도 같은 스위치상에 있는 관리 대상이 되는 모든 서버들의 탐지된 위협 이벤트들을 수집할 수 있다. 이렇게 수집한 이벤트는 실시간으로 분석되어 위협 이벤트들의 위험도에 따라 분류하여 관리 서버의 데이터베이스에 저장된다.

이렇게 데이터베이스에 지속적으로 저장되는 수집/분석된 모든 데이터는 웹 어플리케이션으로 개발 된 내장 IDS기반의 통합 보안관리 시스템을 통해 관리자는 위험도에 따라 분류 된 위협들을 파악하고 해당 위협을 차단 할 수 있다. 관리자가 위협 이벤트를 보고 차단 할 필요성을 느낄 때에 해당 위협을 가한 아이피 주소를 웹상에서 차단하게 되면 IPTable의 정책에 차단할 아이피 주소를 추가

하게 됨으로써 차단이 가능해진다.

3.2 인터페이스 구성

내장 IDS기반의 통합 보안관리 시스템은 웹 어플리케이션으로 개발되어 설치가 불필요하고 웹이 지원되기만 하면 어떤 플랫폼에서든지 접속이 가능하며 동일한 환경을 제공한다. 이것은 관리자가 언제 어디서든 관리자의 역할을 수행 할 수 있다는 것을 의미한다.

4. 구현

내장 IDS기반의 통합 보안관리 시스템은 리눅스 환경에서 작동되도록 구현되었으며, 개발 및 사용 환경은 [표2] 와 같다.

구분	환 경
운영체제	리눅스
개발도구	gcc, editor, Adobe Flex 2
응용프로그램	APM(apache, php, mysql)

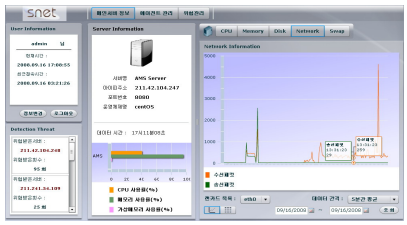
[표2] 개발 및 사용환경

내장 IDS기반의 통합 보안관리 시스템의 인터페이스 개발은 비동기식의 X-Internet 기술이 도입된 Adobe Flex 2 가 사용되었다. 여기서 언급하는 비동기식이란 사용자가 요청을 해서 새로운 데이터를 웹에서 보여줄 때 변경되는 데이터 자체만 불러와서 보여주는 기술을 의미한다. 흔히 웹에서 사용되어지는 PHP나 JSP의 경우에는 새로운 데이터를 가져올 때 마다 전체적인 페이지를 불러와야 하기 때문에 새로운 사용자 입장에서도 시각적으로도 기능적으로도 좋지 않고 서버 입장에서도 과부하를 일으키는 주원인이 된다.

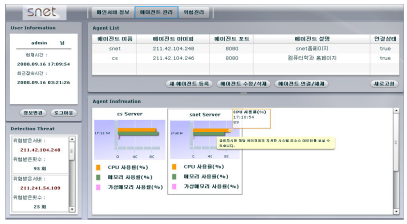
비동기식의 경우에는 처음에 로딩이 끝나면 그 다음부터는 필요시 해당 데이터만 불러올 뿐 화면이 완전히 바뀌어도 페이지를 새로 불러온다거나 하지 않기 때문에 사용자 입장에서 체감속도가 상당히 빨라지게 된다. 또한 지금까지 웹에서는 볼 수 없었던 다양한 효과와 기능들을 웹에서도 구현이 가능하다.

내장 IDS기반의 통합 보안관리 시스템에 로그인 후 첫 화면은 [그림4] 와 같으며 첫 화면에서 관리가 되는 서버들의 위협 받은 횟수와 관리 서버의 시스템 자원 현황을 한눈에 알 수 있다

[그림5] 를 통해서 에이전트가 탑재되어 있는 관리 대상 서버를 추가/변경/삭제가 가능하며 각 에이전트들의 정보와 자세한 시스템 자원 현황을 알 수 있다.[그림6],[그림7] 에서는 관리 대상이 되는 서버들이 받은 위협 이벤트들을 보여주며 각 위협들의 비율을 차트로 알아보기 쉽게 표현해준다. 또한 위협 이벤트의 패킷을 분석하여 표현을 해주며 위협을 가한 아이피의 차단을 할 수 있도록 구현했다.

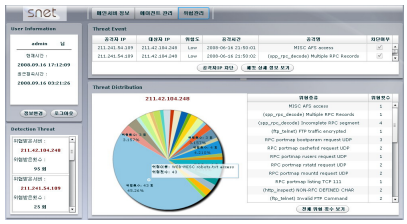


[그림4] 로그인 후 초기 화면



[그림5] 에이전트 관리 화면

[그림6] 위협관리 화면의 패킷 데이터



[그림7] 위협관리 화면의 위협 차트

5. 결론 및 향후 과제

본 논문은 서비스를 제공하는 서버들의 시스템 자원을 감시하여 효율적으로 관리·운영하고 외부의 위협을 원천적으로 차단한 IDS서버를 별도로 두어 관리 대상이 되는 서버들에 대한 위협들을 사전에 탐지하고 차단할 수 있는 내장 IDS기반 통합 보안관리 시스템을 제안하고 구현하였다.

각 관리대상 서버들의 시스템 자원을 관리 서버에 전송받기 위해서는 각각 서버들에 에이전트를 설치해야 하고 내장 IDS가 관리대상 서버들의 위협을 모두 탐지하기 위해서는 관리 서버와 관리대상 서버들이 같은 스위치에 존재해야 한다는 단점이 있지만 관리 서버에서 시스템 자원

을 모두 모니터링하고 위협 탐지 및 차단을 통합적으로 할 수 있다는 매우 큰 장점이 있다.

내장 IDS기반 통합 보안관리 시스템을 사용함으로써 관리대상 서버들을 각각 관리 할 필요가 없어지며 손쉬운 인터페이스로 비보안전문가와 일반 관리자도 쉽게 관리할 수 있다. 내장 IDS기반 통합 보안관리 시스템에서 가장 중요한 점은 IDS가 새로운 위협에 대응할 수 있도록 항상 최신 업데이트 룰을 사용해야 한다는 것이다.

향후 오탐율을 최소화한 IDS가 요구되며 관리대상 서버들을 세부적으로 제어할 수 있는 방법의 연구가 필요하다.

참고문헌

[1] Network and Host-based Vulnerability Assessment, http://www.iss.net/whitepapers/nva.pdf
[2] R. Shirey, Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt, May2000
[3] Susan Cima, Vulnerability Assessment, http://www.sans.org/papers/48/421.pdf
[4] 이강신 외 5명, 네트워크 취약점 점검도구 선정 지침, 한국정보보호진흥원, 2002
[5] 이윤철, 인터넷 보안 기술 및 시장 동향, 정보조사 분석팀, http://dcs.chonbuk.ac.kr/,2004