ESM 시스템간 감사기록 교환방식에 관한 연구

민동옥° 손태식 구원본 문종섭
고려대학교 정보보호기술연구센터
{eieshine°, tsshon, allclear, jsmoon}@cist.ac.kr

A study on the exchange method of audit data among ESM systems

Dong-Og Min° Tae-Shik Shon Won-Bon Koo Jong-sub Moon
CIST, Korea University

요 약

근래 네트워크환경에서 기업네트워크의 보안은 가장 중요하게 고려되고 있는 문제 중 하나이다. 기업네트워크의 보안을 위해 활용하고 있는 VPN, IDS, IPS VDS 등의 다양한 솔루션들은 일관된 관리가 용이하지 않기 때문에 ESM이라는 새로운 대안을 제시했다. ESM은 여러 가지 보안 솔루션을 통합관리 해 주므로, 솔루션의 낭비가 없고 효율적인 관리를 가능하게 하였다. 그러나, 이 ESM들이 가지고 있는 감사 데이터들은 타 ESM들과의 연계가 없기 때문에 독립된 데이터로만 존재하게 되었고, 그에 따르는 한계를 지니게 되었다. 본 논문에서는 이 ESM들의 감사 데이터를 보다 효율적으로 사용하기 위해 타 ESM들과 연계하여 감사 데이터를 교환하는 방식에 대해서 제시하도록 한다.

1. 서 론

급성장하는 근래 네트워크환경에서 대부분의 기업 네트워크들이 인터넷, 인트라넷, 전자상거래 등의 네트워크 시스템 환경을 이용해 전국적이고, 전 세계적인 형태로 확대되어 가고 있다. 이와 같은 기업 네트워크 규모가 증대되면서, 보안상의 취약점을 이용한 기업의 내·외부로부터 발생하는 공격 역시 증가하고 있는 추세이다.

대다수의 기업에서 이러한 공격을 방지하고 대응하기 위하여, 다수의 보안제품을 사용하여 방어하지만 이것을 적절하게 적용시켜서 효과적으로 이용하는데 있어서 많은 어려움을 겪고 있다. 그 이유는 많은 보안정책들을 제품에 맞게 적용시켜야 하고, 보안정책에 따라 보안제품을 어떤 방식으로 적용시키는가에 대한 명확한 해답이 없기 때문이다.

Enterprise Security Management (통합보안관리시스템 : 이하 ESM)은 이런 여러 가지 보안제품들을 적용시키기 위해 개발되었으며, 네트워크 시스템 자원을 분석하고 모니터링하며, IPS, IDS, VPN등의 다양한 보안 솔루션을 통합관리 하여 보안관리의 효율을 극대화시킨다. ESM은 또한 차후에 발생 가능한 침해사고를 예방하고, 증거자료로써 활용하기 위해 IDS나 IPS 등 각 보안 솔루션에서 모여진 감사 데이터를 종합적으로 연계관리하는 기능을 한다.

ESM에서 관리하는 감사데이터는 여러 가지 보안솔루션에서 제공되는 감사 데이터들을 종합하여 분석하여 만들어진 데이터라는 점에서 단일 보안 솔루션에 비해서는 우수한 데이터라고 할 수 있지만, 단일 ESM에서 규합한 데이터라는 점에서 여전히 한계를 가지고 있다. 단일 ESM에서 감사 데이터를 수집하는 ESM은 주변 ESM들이 당한 침해사고나 유행하는 유형의 공격등에 대해서 둔감하게 반응하게 되며, 이로 인해 예방할 수 있는 사고나 공격에 침해당할 수가 있다. 이와 같은 점을 보완하기 위해 각 ESM들은 감사 데이터를 공유해야 하며, 현재 이와 같은 감사 데이터의 공유에 대한 방안에 대하여 제시된 바가 없으므로 본 논문에서 그것을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 ESM이 개요 및 특성에 대하여 설명하고, 3장에서는 본 논문에서 제안하는 감사기록 교환 시스템에 대하여 제시한다. 4장에서는 제시한 시스템에서 파생하는 문제에 대한 해결을, 5장에서는 결론 및 향후 연구방향에 대해서 설명한다.

2. ESM 개요 및 특성

2.1 ESM 전체구조

ESM은 보안정책을 수립하고 수립된 보안정책에 따라서 해당하는 보안 시스템을 구현하며, 이를 모니터링하거나 신속하고 효과적인 조치를 취하기 위해서 각종 경보기능을 제공하는 등의 일련의 작업들을 일관되게 지원해 주는 기능을 한다. 따라서, ESM은 네트워크나 시스템 자원들의 각종 위험요소를 분석하고 모니터링하는 일종의 관리도구로서 IPS, IDS, VDS등 다양한 보안 솔루션들을 통합 관리 해주는 구조를 가지고 있다

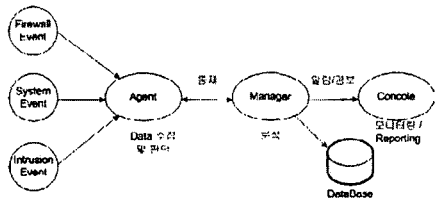

그림 1. 일반적인 ESM 구조

[그림 1]과 같이 ESM은 크게 Console, Manager,

Agent의 구조로 나눌 수 있다. Console은 사용자가 분석과 통계기능, 정책 결정, 이벤트 확인 등을 할 수 있도록 지원해주는 사용자 인터페이스부분이고, Manager는 Agent로부터 수집된 이벤트들을 처리하는 엔진부분이다. 그리고, Agent는 각 보안 솔루션들의 이벤트를 수집, 정규화해서 ESM에서 사용할 수 있도록 가공하는 역할을 한다.

전체적인 ESM의 흐름을 보면, Agent를 통해 수집된 여러 솔루션들의 이벤트를 Manager에서 처리한 뒤, Console에서 그 내용을 확인 하는 구조로 되어있다.

2.2 이벤트 수집 구조

ESM에서 여러 가지 보안솔루션들의 이벤트 수집을 담당하는 부분은 Agent로써, Agent는 이벤트 수집과 Normalize, Aggregation 작업을 거친다. 이벤트 수집은 Collector를 통해서 이루어지며, Collector는 각 보안솔루션에서 발생하는 모든 이벤트를 종합하여 정형화된 데이터로 만들어 낸다.

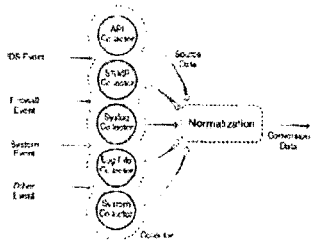

그림 2. Collector의 구조

Collector에서 모아진 각종 데이터들은 수집 카테고리별로 정규화(Normalization) 과정을 거치게 되며, 이러한 과정을 통해 보안솔루션별로 각기 다른 형태로 수집되는 이벤트를 표준화하여 관리할 수 있도록 도와준다. 정규화는 분석이나 알림(Alert)기능을 구현하기 위해 유사한 필드를 갖는 이벤트에 대한 카테고리별로 해당 작업을 수행하게 된다.

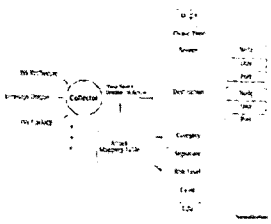

그림 3. IDS에서 발생하는 Event Normalization

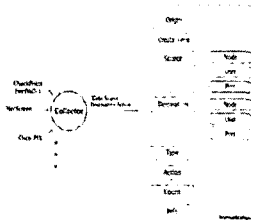

그림 4. IPS에서 발생하는 Event Normalization

정규화 작업을 통해서 얻어낸 결과로, Aggregation 작업을 하여 불필요한 데이터를 제거하고, 중복 데이터를 축약하여 통합관리를 위한 데이터를 수집한다.

3. 제안하는 감사기록 교환 시스템

3.1 제안하는 감사기록 교환 시스템 전체구조

ESM은 Agent에서 얻어진 정형화된 데이터들을 기반으로 분석/반응 하는 시스템이므로, 시스템의 보안을 위해서 많은 데이터와 정확한 데이터가 필요하다. 한 곳의 ESM에서 수집한 이벤트 데이터는 유행하는 유형의 공격이나, 전파되는 특성이 있는 공격 등을 알 수 없기 때문에 주변 ESM들 간의 연계를 통해서 알아내야 한다. ESM들 간의 데이터 공유를 위해서는 각 ESM에 캐시 서버를 하나씩 보유하고 있어야 한다. 캐시 서버는 ESM의 감사기록 데이터를 다른 ESM들이 볼 수 있도록 서비스 한다.

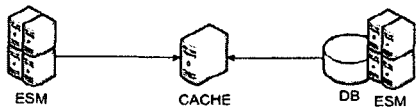

그림 5. 교환을 위한 ESM 단방향 구성도

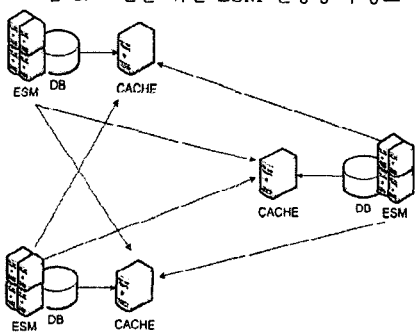

그림 6. 시스템 전체 구성도

한 쪽 ESM에서 본 교환 시스템 구성도는 [그림 5]와 같다. ESM에는 각각 한 개의 캐시서버가 존재하고, 각 ESM은 Aggregation을 거친 데이터가 Manager의 판단을 통해 데이터베이스에 저장되면, 이것을 캐시 서버에서 서비스 할 수 있는 형태로 변환해 캐시 서버에 저장한다. 타 ESM에서 이를 확인하기 위해서는 확인하고자 하는 ESM의 캐시 서버에 접속을 한다. [그림 6]은 단방향 구성도를 여러대의 ESM으로 확장한 것이다.

3.2 감사기록 교환시스템을 위한 ESM 구조

ESM은 일반적으로 3-Tier 구조로 위에서 언급한 Agent, Manager, Console로 되어있으며 그 형태는 [그림 1] 과 같다.

감사기록 교환을 위한 ESM 구조를 만들기 위해서는 기본적인 ESM 구조에 CACHE Agent와 SERVER Agent를 추가해야 한다. 이것은 ESM 구조가 기본적인 구조에서 크게 벗어나지 않는 한 달라지지 않는다.

CACHE Agent는 타 ESM 캐시 서버로부터 데이터를 수집하여 데이터베이스에 전달하여 Manager로 하여금 분석에 사용 될 수 있도록 한다. 이 때, 에이전트에서 수집한 데이터와 CACHE Agent에서 수집한 데이터의 형식이 일치하여 Manager가 데이터 처리에 혼동을 일으키

지 않아야 한다. 그러기 위해서, 캐시 서버에서 제공하는 데이터를 정규화 시켜 CACHE Agent의 수집단계에서 별다른 변환 없이 사용할 수 있게 하였다.

Manager가 분석을 끝낸 후 감사기록을 데이터베이스에 저장하면 SERVER Agent가 정해진 주기로 데이터베이스에 접근해 데이터를 변환시켜 캐시 서버에 저장한다. [그림 7]에 감사기록 교환방식을 위한 ESM의 전체적인 구조가 나와있다.

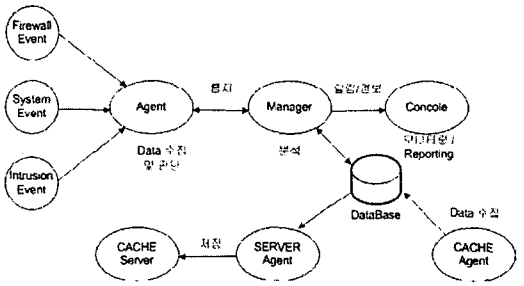

그림 7. 감사기록 교환을 위한 ESM 전체구조

4. 보안과 주기

4.1 주기

ESM에서 발생되는 이벤트와 감사기록이 엄청나게 많은 양이기 때문에, 이 기록들이 데이터베이스에 저장될 때마다 캐시서버에 저장하는 것은 굉장히 비효율적이며 타 ESM에서 캐시서버를 접근하기 난해하게 만든다. 그래서, 일정주기를 두어 SERVER Agent가 주기마다 정해진 파일 이름으로 캐시 서버에 데이터를 보내게 된다. 이 일정 주기는 5분에서 10분을 권장하며, 파일이름은 날짜와 시간의 조합으로 한다. 즉, 2004년 6월 20일 11시 10분의 기록이라면,

http://캐시서버주소/2004/06/20/1110.xml

로 만들어서 제공한다.

CACHE Agent는 Console에서 정해진 정책에 따라 다른 캐시서버에 접근해 데이터를 가져온다.

4.2 보안

4.2.1 캐시 서버 보안

캐시 서버가 제공하는 서비스는 HTTP/HTTPS 프로토콜을 사용한다. 그러므로, 외부에서의 접근 문제가 발생할 수 있고, 이것은 보안상 취약점이 되어버린다. 그러기 때문에, 인증된 ESM 사용자들만 캐시 서버에 접근할 수 있는 인증체계가 갖춰져야 한다.

인증은 허가된 IP 인증과, 계정과 패스워드를 통한 두 가지 인증을 사용하며, 이것은 ESM 관리자 측에서 사전에 협의가 되도록 해야한다. 즉, ESM 캐시서버 테이블에는 자신의 캐시서버에 접속하는 사용자 계정, 패스워드, IP 테이블과 자기가 접속하는 캐시서버의 IP, 사용자 계정, 패스워드 테이블이 존재해야 하며, 이것은 관리자가 용이하게 변경할 수 있게 Console부분에 UI로 지원한다.

4.3.2 데이터베이스 보안

SERVER Agent가 데이터베이스에 접근하여 캐시 서버에 XML 데이터를 생성하는 방법은 크게 두 가지가 있으며, 첫 번째는 캐시 서버에서 직접 데이터베이스를 접근하는 방식이고, 두 번째는 캐시 서버내의 에이전트와 데이터베이스 서버내의 에이전트끼리 통신하는 방식이다.

첫 번째 방식으로 직접 데이터베이스를 접근하려면 데이터베이스의 인증과 보안이 가장 중요하며, 데이터베이스 인증 역시 IP를 통한 인증과 사용자 계정/패스워드를 통한 인증을 병행 사용한다.

두 번째 방식인 캐시 서버 에이전트와 데이터베이스 서버 에이전트끼리의 통신은 에이전트의 통신 프로토콜을 직접 설계하기 때문에, 인증 취약점은 없으나 스니핑의 위험이 있으므로 암호화 통신을 한다. 암호 알고리즘은 3DES, AES, RSA 등을 사용하며, 이 방식에서는 데이터베이스 에이전트로부터 직접 XML 파일이 생성되어 캐시서버로 전송된다.

5. 결론 및 향후 연구방향

ESM에서 수집하는 감사기록 데이터는 공격여부를 판단하는데 가장 기본적인 자료가 된다. 이 감사기록 데이터를 타 ESM들과 교환하여 많은 양의 감사기록 데이터를 보유하게 되면, 아직 침해당하지 않은 새로운 기법의 공격이나, 전파되는 공격에 대해서 능동적으로 대처할 수 있게 된다. 그러나 현재 실제로 사용되고 있는 ESM의 감사기록 데이터의 양은 수시간당 테라바이트 급으로 수집되고 있기 때문에, 본 논문에서 제시하는 교환 방안을 그대로 적용하여 모든 감사 기록 데이터에 대해서 사용할 수는 없다.

이 문제를 해결하기 위해서는 관리자가 감사기록에 대한 등급을 정의하고, 높은 등급 순서의 감사기록만을 교환하는 절제된 감사기록 교환을 해야 한다. 그리고, 사용되는 감사기록의 형식을 일치시켜 ESM이 교환된 감사기록 데이터를 사용하는데 부담을 주지 않아야 한다. 이를 위해서 이후 감사기록의 등급에 대한 기준과 ESM 감사기록 데이터의 형식에 대한 규정이 필요하다.

6. 참고문헌

[1] ISTF-003, IP계층에서의 VPN보안기술 표준, 2003, 3
[2] ISTF-005/R, 침입탐지시스템 로그형식 표준, 2003, 4
[3] ISTF-005/R, 침입탐지시스템 로그형식 표준, 2003, 4
[4] 최양서, 최병철, 서동일, Open Source를 활용한 S-ESM 개발, 한국전자통신연구원,
[5] Symantec, ESM Response Policy Release Notes, 2000, 10
[6] ESM
http://www.kisa.or.kr/K_trend/KisaNews/200011/Esm.html