Light Weighted DB 보안 어플라이언스 개발 사례 연구

The Case Study on Weighted DB Security Appliance Development

서양진*, 이재필*, 이창훈**, 장항배***

Yang-Jin Seo*, Jae-Pil Lee*, Chang-Hoon Lee**, Hang-Bae Chang***

요 약

업무효율 향상을 위해 중소기업에서의 정보시스템 사용이 대중화 되면서 초기 대기업을 중심으로 사용된 DBMS 활용이 중소기업 경쟁력을 강화시키는 데 중요한 촉매제 역할을 하고 있다. 그러나 정보시스템 및 DBMS 확산에 따라 보안사고와 같은 역기능도 함께 대두되면서 대기업에 비해 상대적으로 경영자원이 부족한 중소기업은 보안 시스템에 대한 투자가 미흡하여 DB보안 시스템을 도입하는 데 어려움을 겪고 있다. 따라서 본 논문에서는 중소기업의 DBMS 사용에 따른 해킹 및 보안사고 위협들을 사전에 방지 할 수 있는 중소기업의 정보화 환경에 적합한 간략한 하드웨어 형태의 DB보안 어플라이언스를 설계하고자 한다.

Abstract

SMEs (Small and Medium-sized Enterprise) have become competitive by improvement of work efficiency due to utilization of DBMS, which is mainly used among large enterprises, but reverse functions such as security events and vulnerabilities have been increasing. SMEs without enough investment on security infrastructure have difficulties with implementing DB security products. Therefore the most of SMEs are exposed to hacking and security accidents defensivelessly. Hence this study offers distributional H/W DB security solution which is affordable for SMEs.

Key words : Light Weighted DB Security, SME's DB Security, Security Appliance, Access Control

I. 서 론

인터넷의 발달과 e-비즈니스를 비롯한 전자상거래 등이 활성화 되면서 다양한 정보의 교환과 공유 등이 편리해져 산업의 발달에 도움을 주고 있지만 보안이라는 해결해야 할 큰 문제가 대두되고 있다. 현재까지 많이 고려되고 구축되어온 보안은 통신상 보안(Session Protection)과 시스템 접근 제어(Access Control) 등에 관계된 내용이 대부분이고 궁극적으로 저장되는 가장 중요한 데이터는 평문 상태로 저장되는 형태의 보안이 대부분이었다. 그러나 금전적으로는 시스템의 해킹으로 인한 피해보다 중요한 정보의 유출로 인한 피해가 더 크게 발생한다. 세부적으로 경쟁사의 중요한 정보를 노리는 산업스파이나 이에

* 소프트캠프(주)
** 한경대학교 컴퓨터공학과(Department of Computer Engineering, Hankyoung University)
***대진대학교 경영학과(Department of Business Administration, Daejin University)
· 교신저자(Corresponding Author): 장항배
· 투고일자 : 2010년 3월 19일
· 심사(수정)일자 : 2010년 3월 22일 (수정일자 : 2010년 6월 14일)
· 게재일자 : 2010년 6월 30일

매수된 내부 직원에 의한 경쟁력 있는 노하우의 유출, 그리고 서비스하는 고객들의 개인 신상의 중요한 정보들의 유출 등으로 인한 피해가 더 크다는 것이다[1]. 따라서 주요 정보에 대한 접근 통제 및 감사 시스템 도입이 필수적으로 요구되고 있으며, 이러한 요구사항은 각 분야별 법규와 최근 상정된 개인정보보호법 등을 통해 강제되고 있는 만큼 DB보안 시스템에 대한 기업의 요구사항은 앞으로 더욱 커질 것으로 예상된다[2].

더구나 대기업 중심으로 보급되었던 DBMS가 중소기업의 업무능률 향상과 경쟁력 강화를 위해 확산되면서 중소기업의 DB보안 시스템 도입 요구는 더욱 절실해지고 있다. 그러나 데이터를 관리하고 보호하기 위한 보안시스템이 중소기업 정보화 환경에 부합되지 않으면서 다양한 기능과 높은 가격 등으로 인하여 경영자원이 부족한 중소기업으로써는 상대적으로 데이터의 변경, 손상, 노출 등의 위협에 노출될 수밖에 없는 상황이다. 이러한 상황은 결국 중소기업의 신뢰성에 영향을 끼치는 주요 원인으로 작용되고 있다.

따라서 본 논문에서는 다양한 위협들을 사전에 방지 할 수 있는 중소기업 정보화 환경(개인용 PC 중심의 단순한 정보화 업무처리 환경)에 적합한 간략한 하드웨어 형태의 DB보안 어플라이언스(DB Security Appliance)를 갖춘 설계하고자 한다.

Ⅱ. 관련연구

2-1 네트워크 및 애플리케이션 보안 기술

일반적으로 IT 비즈니스 환경에 대한 보안시스템 구성 요소는 개인 사용자 PC 측면에서는 바이러스 백신, 개인용 PC방화벽, 키보드 보안, 장치 보안 등이 있다. 또한, 네트워크 측면에서는 SSL, PKI, IDS/IPS 등이 있으며, 서버 측면에서는 응용 프로그램 보안, OS보안, DB 보안 등이 개발되고 있다.

보안 시스템 개발수준에 있어서는 개인용 PC 보안 및 네트워크 보안 분야는 이미 오랜 기간 동안 보안 시장에서 기술적 검증을 받아온 부문으로서 현재 대부분의 조직에서 에서나 적용되어 있다. 또한 SSL, PKI 등을 적용한 네트워크 보안부분도 점차 일반화되고 있는 추세이다.

그러나 상대적으로 DB 응용 프로그램 보안 시스템 수준(기술 및 보급측면)은 아직까지 다른 영역의 보안시스템에 비해 상대적으로 미흡한 수준이다.

DB 보안 시스템은 해킹 및 내부자의 불법적인 정보유출을 보호하는 기술을 의미한다. DB 보안 시스템은 내/외부의 권한 있는 사용자에 의한 정보유출 등의 역기능을 사전에 예방하고 혹시나 발생한 사고에 대해서는 사후추적 할 수 있는 감사기능을 가지는 시스템이라고 할 수 있다[4].

2-2 DB 보안의 주요 기술

그림 1. DB 보안 시스템 핵심 기술
Fig. 1. Core Technology of DB Security

DB보안 시스템은 위의 그림 1과 같이 접근 통제, 권한 통제, 사후 추적 등의 핵심 기술로 구성되어 있다[4][5].

접근통제 기술은 인가된 사용자 접근, DBMS 서비스 자체의 결함으로 인한 노출 차단, telnet 및 ftp의 DB 접근 통제 기능을 의미한다. 권한 통제 기술은 사용자별 허가된 SQL 질의어 사용, telnet 및 ftp의 DB 권한 통제 등을 의미한다. 마지막으로 사후 추적 기술은 인가된 사용자의 DB 접근내역 기록, DB 사용내역 기록, 감사 자료생성 등의 기능을 제공한다.

2-3 접근 통제와 권한 통제 특징

그림 2와 같이 DB 보안 시스템은 미들웨어, 웹, 개인 사용자 프로그램 등이 모두 보안영역으로 설정된다.

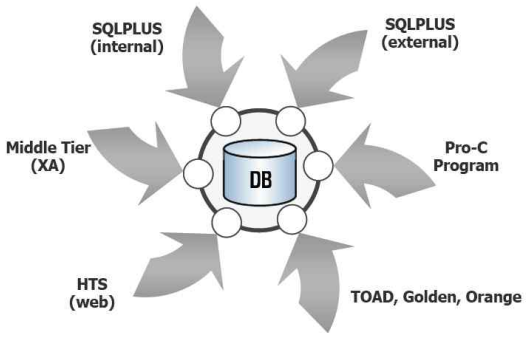

그림 2. DB 보안 시스템 보안 영역
Fig. 2.Security Area of DB Security System

그리고 다음과 같이 DB에 대한 접근 및 권한통제 기능을 기본적으로 가지고 있어야 한다.

① DB 서버의 부하를 전혀 주지 않는 별도의 하드웨어 장비를 이용하여 보안기능 수행

② 기존 DB에서 적용 할 수 없었던 사용자 정보(IP, 접속 AP, 컴퓨터 이름 등)를 이용한 보안정책 수립으로 보안 취약점들을 사전에 예방

Ⅲ. 경량형 DB보안 어플라이언스 설계

3-1 DB보안 어플라이언스 설계 과정

어플라이언스(appliance)장비란 OS, 응용 프로그램 등을 설치 및 설정하지 않고 전원을 공급하면 즉시 사용할 수 있는 정보 단말기기를 의미하며 한다. 기존 소프트웨어 형태의 경우 별도의 관리서버 운영 및 운영을 위한 전문지식을 필요로 하다. 하지만, 하드웨어 일체형 어플라이언스 장비의 경우 소프트웨어 형태에 비해 간단한 조작만으로 서비스 운영이 가능하며, DB보안 서비스를 위한 별도의 인력이 필요하지 않고 간략한 형태의 DB보안기능을 수행할 수 있으므로 경영자원이 부족하고 단순한 형태의 정보화 환경을 가지고 있는 중소기업에게 적합한 형태라 할 수 있다.

그림 3은 DB보안 어플라이언스에 세부적인 동작 과정을 시간 흐름에 따라 정리한 것이다. 서버와 클라이언트 설치 이후 사용자 명령어를 요청하고 DB 보안 어플라이언스에 의해 처리되어 최종적으로 사용자 명령어가 완료된다.

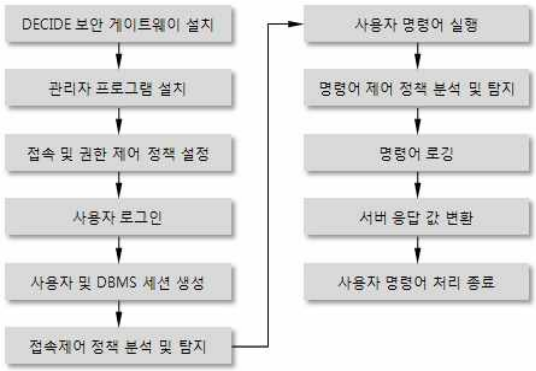

그림 3. DB 보안 어플라이언스 전체 흐름도
Fig. 3. DB Security Appliance Process

3-2 사용자/DBMS 세션 생성

사용자 및 DBMS 세션을 생성하기 위해서는 그림 4처럼 서비스 포트를 통하여 사용자가 접속 요청하면 서비스는 해당 세션에 대하여 전담하는 thread를 생성한 다음 사용자와 보안 대상과의 통신을 중계하며 감사데이터를 수집한다.

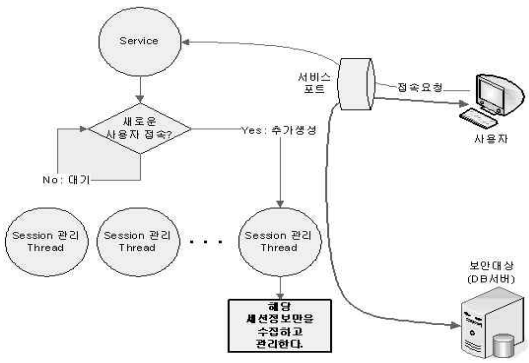

그림 4. 서비스 요청에 따른 세션 생성 흐름
Fig 4. Session Creation Flow upon Service Request

3-3 접속 제어 정책 분석 및 탐지

그림 5와 같이 DB 보안 어플라이언스는 각각의 서비스에 대하여 접근제어정책과 권한정책에 대해서 데이터베이스의 테이블 형태로 유지, 관리하며 서버에 서비스 별로 관련 테이블 내용을 메모리에 적재한다.

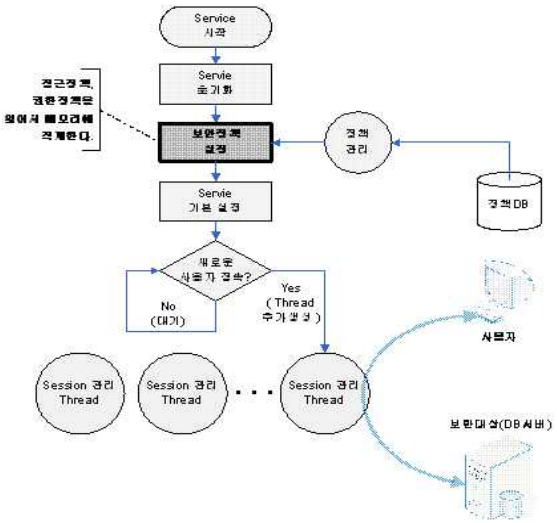

그림 5. 접속제어 분석정책 적재
Fig 5. Loading of Access Control Policy Analysis

그 다음 DB 보안 어플라이언스는 접속 및 권한정책 비교를 위하여 패턴 매칭이나 데이터의 행태분석을 수행한다.

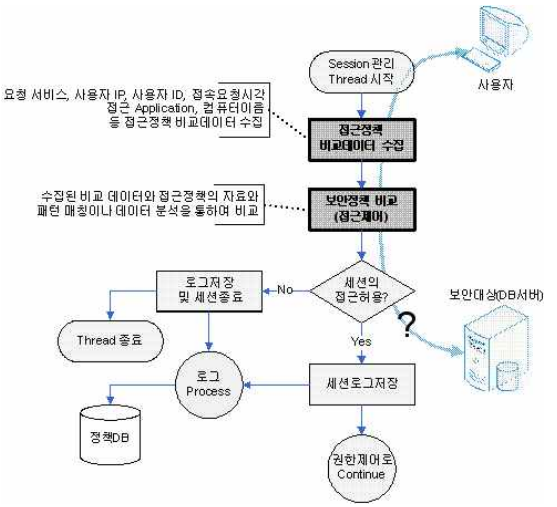

그림 6. 접속제어 정책 비교
Fig 6. Pattern Matching of Access Control Policy Analysis

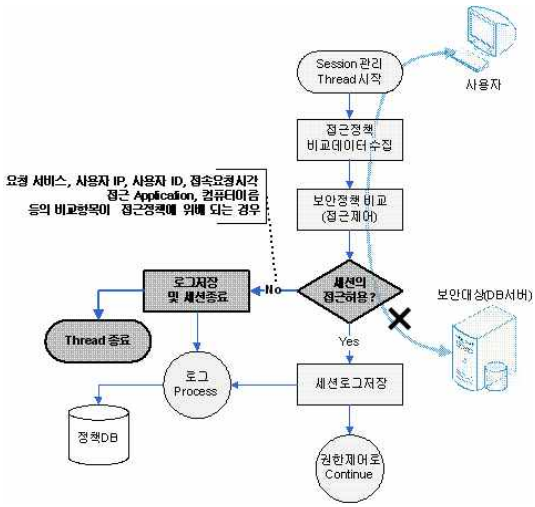

그림 7 접속제어 정책 탐지
Fig 7. Access Control Policy Detection

그림 7과 같이 DB보안 어플라이언스는 감사데이터와 사전에 정의된 접근통제 목록을 확인함으로써, 인가되지 않은 주체의 DBMS 서비스 포트접근에 대하여 보안정책 위반내용을 탐지하게 된다.

3-4 명령어 제어 정책의 분석 및 탐지

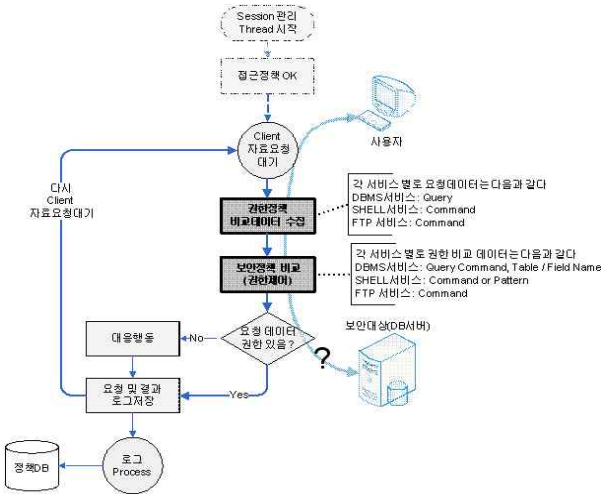

그림 8. 권한제어 정책분석
Fig 8. Authority Control Policy Analysis

그림 8과 같이 접근정책에서 권한이 있어서 접속이 허용되면 서비스는 계속 루핑을 돌면서 사용자의 자료요청에 대한 권한정책을 점검하면서 대응 행동 및 로그를 남긴다. 참고로 이 과정에서 요청되는 데이터는 아래와 같다.

- Query: 사용자 명령어
- 테이블/컬럼: 사용자가 조회하고자 하는 테이블 또는 컬럼
- ID: 사용자 계정
- 애플리케이션: 사용자 응용 프로그램
- IP: 사용자 주소

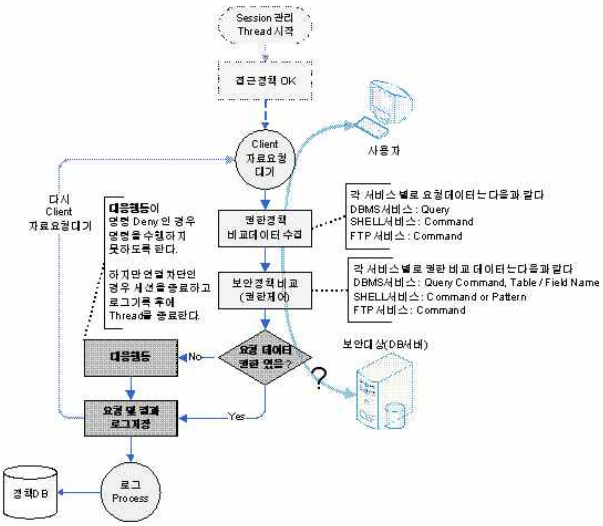

그림 9. 권한제어 정책탐지
Fig 9. Detection of Authority Control Policy

그림 9 권한제어 정책탐지와 같이 DB보안 어플라이언스는 권한정책에서 허가되지 않은 사용에 대해서 보안정책 위반이 탐지된 것으로 판단한다. 그 다음에는 대응행동 및 조치기능을 호출 한다.

Ⅳ. DB보안 어플라이언스 구현

4-1 DB Gateway Agent

사용자 클라이언트는 TCP/IP 프로토콜과 응용 레벨의 오라클 TNS 프로토콜을 이용하여 오라클 DBMS에 접속한다. 이 때 사용자 세션과 오라클 DBMS 사이에 ORACLE DB Gateway Agent가 위치하게 된다[6].

사용자는 Socket을 이용하여 접속 요청하기 때문에 ORACLE DB Gateway Agent는 사용자 세션을 오라클 DBMS로 가장하여 접속을 받아들이게 된다. 그리고 사용자 접속요청과 동시에 오라클 DBMS에 사용자로 가장하여 사용자 대신 ORACLE DB Gateway Agent가 접속하여 양단(사용자와 DBMS 서버)간에 패킷의 중계 역할을 수행하도록 한다.

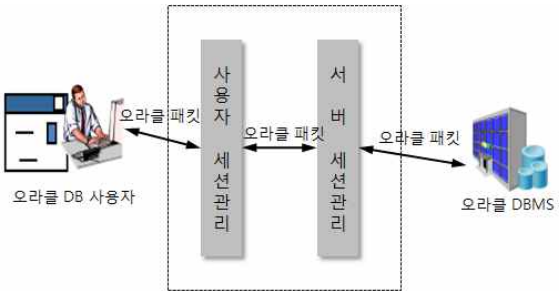

그림 10. DB 게이트웨이 에이전트
Fig. 10. DB Gateway Agent

그림 10과 사용자는 오라클 DBMS에 직접 연결하여 명령어를 실행하는 것과 동일하게 ORACLE DB Gateway Agent는 사용자와 오라클 DBMS 중간에서 패킷의 중계 역할을 수행한다.

4-2 Query Packet Data Parsing Agent

ORACLE 7i, 8i Query Packet Data Parsing Agent는 오라클 DBMS의 버전을 의미하며, 현재 9i, 10g가 가장 널리 보급되어 있다. 동일하게 오라클 TNS 프로토콜을 사용하지만, 이전 방식의 오라클 TNS 프로토콜과 최신의 TNS 프로토콜과는 많은 차이점을 가지고 있다.

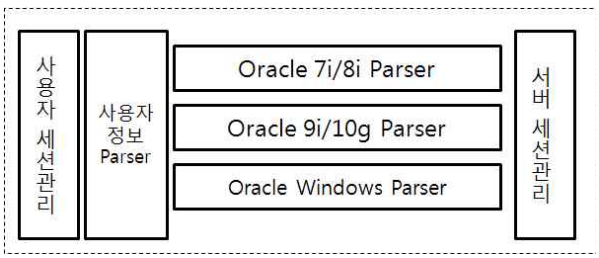

그림 11. ORACLE 질의어 파싱 에이전트
Fig. 11. ORACLE Query Packet Data Parsing Agent

Parsing Agent는 4개의 Parser로 구성된다.

① 사용자 정보 Parser

사용자 로그인 시 사용자 정보를 포함한 로그인 패킷이 서버에 전송된다. 이 때 사용자 정보를 얻기 위한 Parser로써 아래와 같은 정보를 패킷에서 추출한 후 모니터링, 로그 기능을 동작하며 DB보안 서버 엔진 모듈에 전송하여 처리를 할 수 있도록 한다. 여기서 사용되는 사용자의 주요정보는 아래와 같다.

- 로그인 ID: 오라클 DBMS 로그인 ID
- 사용자 응용 프로그램: 예를 들어 Toad, Golden, SQL Plus 등
- 컴퓨터 이름: 사용자 host 이름
- OS ID: 사용자 OS ID
- 사용자 IP
- 로그인 시간

② Oracle 7i/8i/9i/10g Parser

오라클 DBMS 서버가 7i/8i일 경우 TNS Protocol Parser로써 9i/10g와는 차이점이 있다. 예를 들어, 사용자 명령어의 시작 부분의 위치, 길이 정보 등이 없는 경우가 발생하여 이에 해당되는 TNS Protocol을 분석하기 위한 Parser이다.

③ Oracle Windows Parser

오라클 DBMS 서버의 OS가 Windows 일 경우는 일반적인 서버 접속의 방법과 같이 1521 port(오라클 DBMS default port)로 접속 후 1521 port와의 세션을 계속 유지하는 것이 아니라, 접속 로그인 후 새로운 port를 오라클 서버로부터 할당받아 재 연결을 시도하는 경우이다. 이 때 1521 port를 통해 서버에 접속하는 접속하도록 유도 또는 감지하여 Parser를 수행하는 parser이다.

4-3 DATABASE 보안정책 처리 AGENT

관리자 프로그램에 의해 설정된 정책 항목들을 정책이 저장된 DB에서 읽어 메모리에 적재토록 하는 모듈로써 Policy Manager라 칭한다.

Policy Manager는 관리자에 의해 정책이 추가/변경/삭제되었을 경우 기존의 적재되어있던 정책을 삭제하고 재 적재토록 하는데, 명령어 처리 중에 사용자 lock을 걸고 안정하게 변경된 정책이 수행토록 동기화(synchronization) 기법을 이용하여 처리된다.

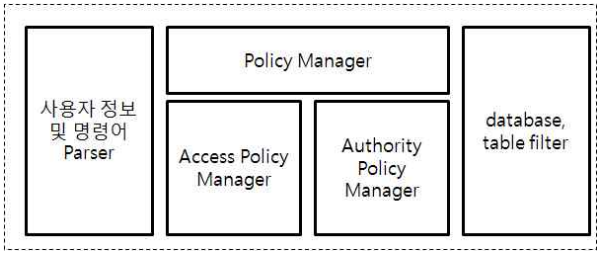

그림 12. 정책 제어 모듈 구성도
Fig. 12. Structure of Policy Control Module

그림 12와 같이 ORACLE Query Packet Data Parsing Agent로부터 추출된 정보를 Policy Manager를 통해 각각의 정책에 부합되는지 점검하기 위한 Access Policy Manager, Authority Policy Manager 및 Database, Table, Filter 모듈 등으로 구성된다.

4-4 DATABASE TABLE QUERY FILTER

Database Table Filter 모듈을 의미하는 것으로, 사용자 정보 및 명령어 Parser에 의해 추출된 사용자 명령을 정책에 의해 Database, Table, Column의 정확한 위치 및 특정 Column 포함여부 등을 판단하기 위한 모듈이다. Alias 추출, Nested 구문 파악 등의 구분분석 기능을 포함하고 있다.

4-5 DATABASE 접근 및 권한 제어 AGENT

그림 13은 서버 모듈 구성을 나타내고 있으며 대략적으로 사용자 접속 및 명령어 제어 등의 기능을 수행하게 되며, ID, Application, Computer 이름, IP 및 사용자 명령어를 Database Table Filter 모듈과 연동하여 제어를 수행하는 모듈이다. 이 때 기능하는 모듈은 Access Policy Manager, Authority Policy Manager 등의 2개 모듈로 구분한다.

그림 13. 서버 모듈 구성도
Fig 13. Structure of Server Module

4-6 AGENT 보안정책 설정

사용자 통제에 필요한 항목은 표 1 보안 정책 Object List와 같은 항목으로 Object를 설정하고 설정된 Object를 바탕으로 보안 정책을 설정할 수 있는 정책 처리를 수행한다.

표 1. 보안정책 Object List
Table 1. Object List of Security Policy

Object	내용
접속IP	IP를 보안정책의 Object로 활용
사용자 ID	ID를 보안정책의 Object로 활용
컴퓨터 이름	컴퓨터 이름을 보안정책의 Object로 활용
사용 응용 프로그램	사용 응용 프로그램을 보안정책 Object로 활용
시간 정보	시간을 보안정책의 Object로 활용
대기 시간	IP를 보안정책의 Object로 활용

4-7 로그분석 및 조회

표 2 로그 조회 항목과 같이 IP, 컴퓨터 이름, ID, 애플리케이션, Table, DMS, Query 응답시간, Telnet 사용자, 명령어 별 조회 조건을 통해 로그 조회를 수행한다.

표 2. 로그 조회 항목
Table 2. Log Reference Items

종류	내용
IP 별 사용 내역 조회	사용자 IP를 이용한 조회, 검색 기능 제공
단말기 이름을 이용한 조회	사용자 컴퓨터이름을 이용한 조회, 검색 기능 제공
ID를 이용한 조회	사용자 Oracle ID를 이용한 조회, 검색 기능 제공
애플리케이션별 조회	사용자가 DB접속에 사용한 Application을 기준으로 조회, 검색 기능 제공
TABLE 액세스를 이용한 조회	액세스 대상 TABLE를 기준으로 QUERY나 사용자를 조회, 검색하는 기능 제공
DML 기준 조회	DML 명령을 기준으로 사용자를 조회, 검색하는 기능 제공
SQL Query 응답시간 조회	SQL Query를 실제 질의에서 응답까지의 시간 조회 기능

실시간으로 DB보안 어플라이언스 서버 모듈로부터 현재 접속되어있는 사용자의 명령어 수행 및 결과를 표 3의 항목에 의거해 조회한다.

표 3. 실시간 사용자 세션 조회 항목
Table 3. Session Reference Items of Real-Time User

종류	내용
접속IP	접속IP 별 QUERY 검색 및 상세정보 제공
사용자 ID	사용자 ID 별 QUERY 검색 및 상세정보 제공
컴퓨터 이름	컴퓨터 이름 별 QUERY 검색 및 상세정보 제공
사용 애플리케이션	사용 애플리케이션 별 QUERY 검색
시간 정보	시간대별 IP 현황, 시간대별 사용자
상세 검색기능	현황 등의 정보제공 및 상세 검색기능
응답 시간	평균 응답시간 및 응답시간 등의 기타
검색	검색어 입력을 통한 조회

Ⅴ. DB보안 어플라이언스 실행결과

앞서 설명한 DB보안 어플라이언스에 대한 설계 및 구현과정에 따라 최종적으로 구성된 내용은 표 4와 같으며, 이에 따른 동작 흐름은 표 5와 같이 정리 될 수 있다.

표 4. DB보안 어플라이언스 핵심모듈
Table 4. Major Core Module of DB Security Appliance

구성요소	설명
사용자 세션 관리	사용자와 오라클 DBMS 사이에 Gateway 역할로써 사용자 세션과 오라클 DBMS 세션에 대한 패킷의 중계 역할을 수행
사용자 정보 및 명령어 Parser	사용자의 로그인 정보 및 사용자 명령어 정보를 오라클 TNS 프로토콜 패킷으로부터 추출
Access/Authority Policy 관리자	사용자의 접속 또는 명령어 사용에 대한 제어 담당
관리자 지원	관리자 프로그램으로써 세션 모니터링, 로그 조회, 권한 설정 등의 기능을 제동

표 5. 사용자 세션과 DBMS 서버 사이의 통신 관계
Table 5. Communication Relationship between User Session and DBMS Server

통신 순서	비고
사용자 → DB보안 어플라이언스	사용자 Send 내용을 평가시스템 Socket으로 Receive
DB보안 어플라이언스 → DBMS 서버	사용자 Send내용을 DB서버에 Send
DB보안 어플라이언스 ← DBMS 서버	DB서버 Send내용을 평가시스템이 Socket으로 Receive
사용자 ← DB보안 어플라이언스	DB서버 Send내용을 사용자에게 Send

5-1 사용자 세션 관리

사용자는 DB 보안 어플라이언스 장비를 통하여 DBMS서버에 접근하게 되는데 이때 서비스에 등록된 포트별로 서비스를 하면서 사용자가 보안대상인 DBMS서버로 접근하는 자료를 수집한다. 해당 포트를 Socket으로 Open하여 데이터가 유입되면 이를 해당 서비스에 대한 접속 요청인지 확인하고, 이에 대하여 연결 유지 및 유입 데이터를 수집하여 메모리상에 임시 저장한다.

세션 관리 모듈에서 직접 사용자와 DBMS 와의 세션을 맺고 패킷을 중계하기 때문에 사용자 명령어에 대한 패킷 손실이 전혀 발생하지 않아 안정적으로 기능을 수행할 수 있다. 참고로 세션 데이터의 수집방법은 범용적인 Socket 통신을 통하여 사용자 세션과 DBMS 서버 사이의 통신을 수집하여 세션을 관리한다.

5-2 사용자 정보 및 명령어 Parser 모듈 실행 및 분석

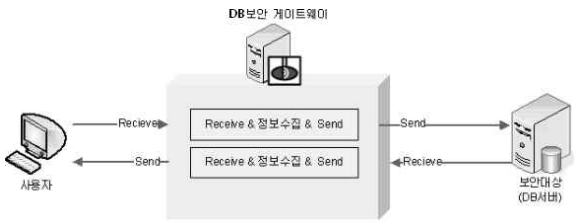

그림 14. 사용자 세션과 DBMS 서버와의 세션 관리
Fig. 14. Session Management of User Session and DBMS Server

그림 14처럼 사용자 세션과 DBMS 서버와의 세션 관리를 위하여 사용자 정보 및 명령어 Parser 모듈은 사용자 세션 관리 모듈에서 연결된 사용자와 DBMS 사이의 중계되는 패킷을 Parsing하여 사용자 정보와 사용자 명령어를 추출한다.

① 사용자 정보 Parser

그림 15의 사용자 정보 Parser와 정책 모듈을 연동처럼 사용자의 정보의 추출은 ID, 애플리케이션, 컴퓨터 이름, OS ID등의 정보를 오라클 DBMS 로그인 시의 패킷을 이용하여 얻어낸다.

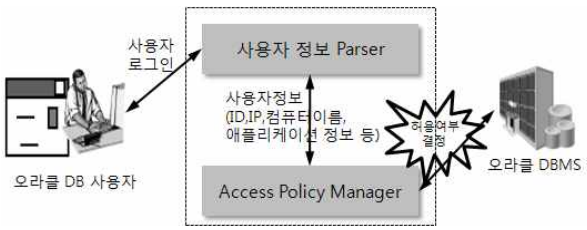

그림 15. 사용자 정보 Parser와 정책 모듈 연동
Fig. 15. Inter-working of User Information Parser and Policy Module

사용자 정보를 추출하여 메모리에 저장하게 되면 Access Policy Manager 모듈에 의해 관리자에 의해 허용토록 설정된 사용자인지 확인하여 접속을 차단/허용 등의 동작을 수행한 한다.

아울러 사용자의 정보는 2종류의 패킷을 이용하여 얻어낸다. 첫째는 그림 16 사용자 로그인 정보 패킷 유형 1에서처럼 최초 로그인 시 DBMS 서버에게 자신의 정보를 알리기 위한 패킷으로 해당 문자열을 파싱하여 IP, 사용자 응용 프로그램 이름, 컴퓨터이름 등을 얻어온다.

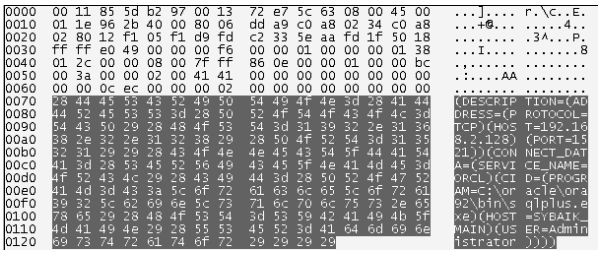

그림 16 사용자 로그인 정보 패킷 유형 1
Fig. 16. User Login Information Packet Type 1

둘째로, 위의 패킷에서 얻지 못한 사용자 ID를 구하기 위해 그림 17에서 처럼 사용자 로그인 정보 패킷 유형 2를 이용하여 사용자 ID, 컴퓨터 이름 등을 추출해낸다.

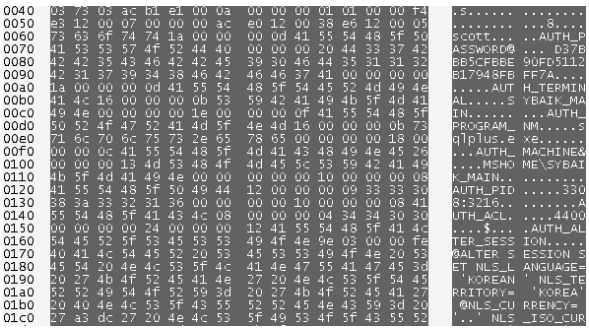

그림 17 사용자 로그인 정보 패킷 유형 2
Fig. 17. User Login Information Packet Type 2

② 사용자 명령어 Parser

그림 18의 사용자 명령어 Parser와 정책 모듈과의 연동처럼 사용자 명령어를 포함한 패킷일 경우 오라클 TNS 프로토콜에 의거하여 분석하여 명령어를 추출한다.

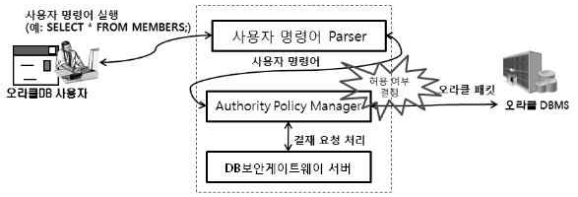

그림 18. 사용자 명령어 parser와 정책 모듈과의 연동
Fig. 18. Inter-working of User Command Parser and Policy Module

추출된 명령어는 Authority Policy Manager 모듈과 연동하여 접근 허가된 명령어인지 판단하여 DB 보안 어플라이언스 서버 모듈에게 전송한다. 그 다음 사용자 명령어가 허용으로 설정되어 있는 정책이었을 경우 DBMS 서버로 패킷을 전송하여 정상적으로 명령어를 수행하도록 한다.

만약 사용자 명령어가 차단으로 설정되어 있으면 해당 명령어를 변조하여 DBMS 서버로 패킷을 전송토록 한다. 이 때 변조된 명령어는 DBMS 서버에서 인식할 수 없으므로 사용자 명령어는 실행되지 않게 된다.

5-3 Access/Authority Policy 관리

이 부분은 정책을 메모리에 보관하는 Policy Manager와 접속 정책을 담당하는 Access Policy Manager 및 명령어 제어 정책을 담당하는 Authority Policy Manager로 구성한다.

① Policy Manager

관리자에 의해 설정된 정책을 메모리에서 보관하고 정책이 변경되면, 해당 정책의 동기화 기법을 이용하여 정책이 적용되도록 한다. 수신된 정책은 Access/Authority Policy Manager에게 정보를 전송하여 각각 정책을 수행토록 한다.

② Access Policy Manager

사용자의 오라클 DBMS 서버 로그인 시 해당 접속 허용/차단 여부를 결정하며, 접속 정책을 비교하는 항목은 아래와 같은 Object를 이용한다.

- 접속IP: IP 및 IP 그룹을 보안정책의 Object로 활용할 수 있다.
- 사용자 ID: ID를 보안정책의 Object로 활용 할 수 있다.
- 컴퓨터 이름: 사용자 컴퓨터 이름을 보안정책의 Object로 활용 할 수 있다.
- 사용 Application: 사용 애플리케이션 및 그룹을 보안정책의 Object로 활용 할 수 있다.
- 시간 정보: 날짜 범위 또는 시간 범위를 보안정책의 Object로 활용 할 수 있다.
- 관리자 경고 설정 사항: 해당 정책에 만족할 경우 특정 대상 또는 그룹에게 메일, SMS, 관리자 프로그램을 통한 화면 디스플레이 설정을 통해 사건을 알리도록 설정한다.
- 접속 설정 사항: 상기 Object를 만족하면 허용 또는 세션의 차단으로 설정한다.

③ Authority Policy Manager

로그인 한 사용자가 명령어를 수행하면 해당 명령어가 허용/차단 명령어인지, 결재 요청 대상 명령어인지 정책 비교를 수행한다. 이 때 권한 정책을 비교하는 항목은 아래와 같은 Object를 이용한다.

- 접속 IP: IP 및 IP 그룹을 보안정책의 Object로 활용 할 수 있다.
- 사용자 ID: ID를 보안정책의 Object로 활용 할 수 있다.
- 컴퓨터 이름: 사용자 컴퓨터 이름을 보안정책의 Object로 활용 할 수 있다.
- 사용 Application: 사용 애플리케이션 및 그룹을 보안정책의 Object로 활용 할 수 있다.
- 일반 명령어, 테이블 및 컬럼, DML, DCL, DDL 명령어를 설정한다.
- 시간 정보: 날짜 범위 또는 시간 범위를 보안정책의 Object로 활용 할 수 있다.
- 관리자 경고 설정 사항: 해당 정책에 만족할 경우 특정 대상 또는 그룹에게 메일, SMS, 관리자 프로그램을 통한 화면 디스플레이 설정을 통해 사건을 알리도록 설정한다.
- 접속 설정 사항: 상기 Object를 만족하면 허용 또는 명령어만 차단, 세션의 차단, 결재 요청 사항을 설정한다.
- 결재 유형 설정: 관리자에 의해 승인 요청, 자동으로 결재 승인 처리, 자동으로 결재 거부 처리, 타임 아웃을 통하여 설정한다.

5-4 관리자 지원 모듈

이 부분은 관리자 프로그램에 의해 모니터링 된 내역에 대한 로깅 조회 등의 기능을 수행하는 DB 보안 어플라이언스 장비의 서버 관리자 지원 프로그램을 의미한다.

- AGENT 보안정책 설정/ 로그조회기능을 수행한다.
- LOG 분석을 통한 REPORT , 각종 정책설정을 위한 로그 조회 기능을 수행한다.
- 현재 사용자 세션 관리 및 특정 QUERY 분석 로그 조회 기능을 수행한다.
- 결재 관리자/담당자 계정관리 및 권한 관련 부분의 정책 설정 기능을 수행한다.
- 결재 상태 및 진행 사항 보고 내용을 실시간으로 확인 가능하다.

5-5 연구 결과 및 평가

본 연구결과로 개발된 DB 보안 어플라이언스 장비는 그림 19와 같으며, 이 장비에 대한 성능평가는 표 6과 같다. 참고적으로 평가요소는 보안성, 기능성, 편리성 등을 대상으로 조작적 변수를 설계하여 충족 여부를 측정하였다. 측정결과 소프트웨어 중심의 DB 보안시스템 기능과 동일하게 성능을 보이고 있음을 확인하였다.

그림 19 하드웨어 형태의 DB 보안 어플라이언스 장비
Fig. 19. Hardware Typed DB Security Appliance

표 6. DB 보안 어플라이언스 장비 성능평가 결과
Table 6. Experiment and Evaluation of DB Security Appliance

평 가 항 목		
구분	항목	기능/성능수준
보안성	실시간 모니터링	현재 접속 중인 DBMS 사용자 모니터링 충족
	세션 정보 로깅	DBMS 사용자의 세션 정보 로깅 충족
	명령어 로깅	사용자의 SQL 명령어 로깅 기능 충족
	사용자 제어	ID, IP, 응용 프로그램에 의한 허용/차단 기능 충족
	명령어 제어	· DML, DCL, DDL 명령어 허용/차단 여부 · ○IP, 컴퓨터이름, 테이블, SQL명령 단위 제어 · 응용프로그램, 시간, 테이블, SQL명령 단위 제어
기능성	Bypass	장애 발생시 Watch Dog 알고리즘을 이용, 물리적으로 새로운 네트워크 경로를 생성하여 사용자 서비스 유지하도록 하는 기능 충족
	Inline	사용자와 서버 사이에 장비가 직렬로 설치되도록 하여 네트워크 구성 변경 없이 설치, 운영할 수 있도록 하는 기능 충족
	스트레스	초당 1000 개의 DBMS SQL 질의어 성능 지원
편리성	관리자 지원	셋업 파일을 이용한 관리자 프로그램의 간단한 설치
		DB 보안 관리자용 응용 프로그램 충족 · 정책 관리(서비스, 접속 및 명령어 제어) · 실시간 모니터링 · 로그 조회 · 관리자 설정(계정 및 패스워드 관리) · 통계 리포트 산출

참고적으로 개발된 보안장비는 모든 SQL 질의어에 에 대하여 세션 유실 없이 보안 기능 수행을 하면서, 사용자 실수로 비인가 명령 수행 시 비인가 명령만 차단하고 세션은 유지하는 가용성도 함께 지원하고 있다.

Ⅵ. 결 론

본 논문에서는 TCP/IP Socket Layer 기반 기술에 의거하여 동작되는 ORACLE의 기존 속도 및 성능을 최대한 저하시키지 않고 ORACLE 접근통제와 질의 명령의 정책에 의한 차단 등의 기능을 하는 경량 형 DB보안 어플라이언스 장비를 제시하였다.

경량 형 DB보안 어플라이언스 장비는 TCP/IP 상에서 진행되는 데이터베이스에 요청되는 사용자의 질의 중 중요 정보에 접근하거나 시스템 관리자만이 접근하는 질의어에 대하여 해당 최종 관리자 또는 중간 관리자에게 정보를 제공함으로써 해당 질의어에 대한 허용여부를 판단, 결정하도록 하며 이를 기록하여 로그로 남기고 관리할 수 있도록 하였다.

본 논문에서 제시된 DB보안 어플라이언스 장비는 시스템은 다음과 같은 의의를 가지고 있다. 먼저 연구적인 측면에서는 현재 소프트웨어 중심의 DB보안 시스템에 비해 간략하고 사용자 수용성이 높은 하드에어 형태의 DB 보안 장비를 어플라이언스 형태로 개발하였다. 둘째, 경제적인 측면에서는 기존에 사용되고 있는 고가의 DB보안 시스템을 경영자원이 부족한 중소기업이 도입할 수 있도록 보안기능을 최적화함으로써 중소기업에 보급이 가능하게 하였다. 마지막으로 관리적인 측면에서는 소프트웨어 형태의 경우 별도의 관리서버 운영 및 운영을 위한 전문지식을 필요로 하지만, 하드웨어 일체형 어플라이언스 형태의 간단한 조작만으로 보안 서비스 운영이 가능하게 함으로써 보안역량이 부족한 중소기업에게 적합하도록 구현하였다.

본 연구의 결과물은 조직 내 첨단 기술에 대한 불법적인 자료 유출을 방지하고자 하는 조직(예를 들면 조선, 반도체, 자동차 등의 제조업체 등), 연구개발 자료에 대한 기밀성을 보호하고자 하는 조직(예를 들면 공공연구기관, 게임 개발업체 등), DBMS와 연동하여 인트라넷 시스템 내 중요 설계 및 개발정보를 보호하고자 하는 조직 등에 응용이 가능할 것이다.

향후 연구로는 비즈니스 프로세스 특성을 고려하면서 다양한 DBMS(예를 들어, 중소기업 전용 DBMS)를 지원할 수 있는 서비스 형태의 DB보안 기술개발이 필요하다.

참 고 문 헌

[1] D. F. Ferraiolo, Role-Based Access Control, Artech House, Computer Security, 2003.

[2] H. G. Lee, S. M. Lee, T. Y. Nam, "Database Encryption Technology and Current Product Trend," *Electronics and Telecommunications Trend Analysis, vol.22, no.1*, pp.105-113, 2007. (In Korean)

[3] M. A. Jeong, J. J. Kim, Y. Won, "A Flexible Database Security System Using Multiple Access Control Policies," *LNCS 2736, pp.876-885*, 2003.

[4] S. Y. Kim, G. W. Nam, S. C. Kim, "Filtering Unauthorized SQL Query By uniting DB Application Firewall with Web Application Firewall,"

[5] Y. Elovici, R. Waisenberg, E. Shmueli, and E.Gudes, "A Structure Preserving Database Encryption Scheme," *Proc. of the Secure Data Management in a Connected World 2004 (SDM 2004),* NCS 3178, pp.28-40, 2004.

[6] D. Keesling, J. Womack, Oracle9i Database Administration Fundamentals II, Production 2.0, D37492, Oracle Corporation, 2002.

서 양 진 (徐良進)

1994년 2월 : 중앙대학교 컴퓨터공학과 (학사)
1998년 2월: 중앙대학교 컴퓨터공학과 (석사)
2006년 2월 : 중앙대학교 컴퓨터공학과 (박사 수료)
2002년~2003년 : 아시안사인(주) 전자거래연구원 팀장
2004년~현재 : 소프트캠프(주) 정보보안기술연구소 팀장
관심분야 : 정보보안, 시맨틱 기술, 정보검색, 인공지능

이 재 필 (李載泌)

1993년 2월 : 중앙대학교 전자계산학과 (학사)
1995년 2월 : 중앙대학교 컴퓨터공학과 (공학석사)
1999년 8월 : 중앙대학교 컴퓨터공학과 (공학박사)
1998년 12월 : 미래산업㈜ 선임연구원
1999년 7월~현재 : 소프트캠프㈜ 부사장
관심분야 : 정보보안(e-DRM,DB보안),인공지능(학습 및 추론)

이 창 훈 (李昌勳)

1987년 2월 : 광운대학교 전자계산학과 (이학사)
1989년 2월 : 중앙대학교 대학원 전자계산학과 소프트웨어공학전공(이학석사)
1998년 2월 : 중앙대학교 대학원 컴퓨터공학과 소프트웨어공학전공(공학박사)
2002년~현재 : 한경대학교 컴퓨터공학과 교수
관심분야 : 객체지향 설계, 컴포넌트, 정형화 명세, 영상처리(증강현실)

장 항 배 (張恒培)

2006년 2월 : 연세대학교 정보시스템 박사
2007년 3월~현재 : 대진대학교 경영학과 조교수
관심분야 : 산업보안, u 비즈니스 전략, 정보화(정보보호) 수준 및 성과평가