韓國컴퓨터情報學會 論文誌
第14卷 第4號. 2009. 4.

2009-14-4-4-3

DB 보안의 문제점 개선을 위한 보안등급별 Masking 연구

백 종 일*, 박 대 우**

A Study on DB Security Problem Improvement of DB Masking by Security Grade

Jong-Il Baek*, Dea-Woo Park**

요 약

오라클 DBMS의 8i버전에서는 암호화 모듈이 기본적으로 장착되어 있으나, 암호화 모듈은 성능저하가 야기되어 제한적으로 적용되고 있다. 본 논문에서는 인덱스검색, 객체관리 혼란, 암호화로 인한 심각한 DB 성능 저하, 실시간 데이터 암호화 미지원, IP기반의 데이터 접근제어 미지원으로 인한 기술별로 DB 보안의 문제점을 분석한다. 그리고 DB 보안의 가용성을 향상시키기 위해 암호화기술의 대체수단인 DB Masking 기법을 활용한 종합적인 보안 프레임워크를 제안한다. 취약점 개선안으로 가상계정을 이용하여 보안등급별로 DB Masking 기준을 설정하고, 가상계정을 통한 사용자 인증과 SQL문의 사전, 사후 결재 및 무결성을 체크하고, 감사 로그로 수집하여 DB를 안전하게 관리 할 수 있는 방안으로 활용한다.

Abstract

An encryption module is equipped basically at 8i version ideal of Oracle DBMS, encryption module, but a performance decrease is caused, and users are restrictive. We analyze problem of DB security by technology by circles at this paper whether or not there is an index search, object management disorder, a serious DB performance decrease by encryption, real-time data encryption beauty whether or not there is data approach control beauty circular-based IP. And presentation does the comprehensive security Frame Work which utilized the DB Masking technique that is an alternative means technical encryption in order to improve availability of DB security. We use a virtual account, and set up a DB Masking basis by security grades as alternatives, we check advance user authentication and SQL inquiry approvals and integrity after the fact through virtual accounts, utilize to method as collect by an auditing log that an officer was able to do safely DB.

▸ Keyword : DBMS, DB Masking, Access Control, virtual account

• 제1저자 : 백종일(jibaig101@empal.com) 교신저자 : 박대우(prof1@paran.com)
• 투고일 : 2009. 03. 09, 심사일 : 2009. 04. 16, 게재확정일 : 2009. 04. 20.
* 호서대학교 벤처전문대학원 IT응용기술학과 **호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

데이터베이스 보안을 위한 핵심적인 기술은 데이터베이스(DB)를 암호화하는 기술이다. 데이터베이스 암호화란 데이터베이스 내부의 데이터 자체를 암호화하는 기술이다. 암호화 기술은 특히 내부자로부터 데이터를 보호할 수 있다는 면에서 장점이 있는 기술이다.

그러나 대부분의 DB 암호화 방식은 소프트웨어 방식으로 DB서버 내에 설치되며, 운용시에 DB서버의 성능을 상당히 떨어뜨리기 때문에 그 효용성이 감소되는 것이 사실이다. DB 암호화 기능을 적용한 상태와 적용하지 않은 상태를 비교했을 때 DB 용량과 스펙에 따라서, 적게는 수 배 에서 많게는 수십 배 이상의 성능 저하를 가져온다.

지금까지 이 문제의 해결을 위한 성능 문제를 개선하기 위해 연구된 하드웨어 제품의 경우에도 초당 쿼리 수의 제한 때문에 ISP, 포털 및 게임 사이트 등에 적용할 만한 대용량 DB 암호화 기술구현 방안은 어려운 실정이다.

국내외 DBMS 시장을 상당수로 점유하고 있는 오라클DB의 경우, 8i버전 이상에서는 암호화 모듈이 기본적으로 내부에 장착되어 있으나, 암호화 모듈을 이용하는 경우 성능저하가 야기되어, 실제 사용자들은 암호화 모듈의 사용을 제한적으로 적용하고 있다.

이 문제로 인하여 DBMS의 성능을 유지하며(가용성) 데이터베이스 자체를 원천적으로 보호(기밀성)하여 내부자 또는 외부에서의 개인정보 불법 획득을 체계적으로 차단할 수 있는 DBMS의 관련 기술 개발이 시급히 요구된다.

본 논문의 연구에서는 각각의 기술별로 DB 보안을 적용했을 때 발생할 수 있는 문제점을 분석하고, DB 보안의 가용성을 향상시키기 위해 암호화기술의 대체수단인 DB Masking 기법을 활용한 종합적인 보안 프레임워크를 제시 한다. 본 논문에서는 가상계정을 이용하여 보안등급별로 DB Masking 기준을 설정하고, 이를 감사(Auditing)로그로 수집하여 DBMS의 가용성 확장과 기밀성을 강화하여 우리나라의 IT 정보사회 발전에 기여하고자 한다.

Ⅱ. 관련 연구

본 장에서는 개인정보 유출 사고 사례를 통한 DB 보안의 필요성과 DB 보안 기술에 대해 살펴본다.

1. 개인정보 유출 사고

2008년도에는 대형 개인정보유출 사고가 총 세 차례나 일어났다. 표 1과 같이 2008년 2월에는 인터넷 경매사이트 옥션에서 해킹사고가 발생해 총 1,081만명의 개인정보가 유출됐다.[11] 또한 하나로텔레콤에서는 고객정보 600만명이 텔레마케팅용으로 무단 사용되는 일이 발생했다. 8월에는 GS칼텍스 내부정보 유출사건은 권한 있는 내부직원이 금품을 목적으로 일어난 사건으로 보다 강력한 DB 보안의 안전성을 위협하는 사고가 발생하였다.[12]

2008년 유출된 정보 건수는 2,800만명 분량으로 단순 계산상으로 우리나라 전체인구의 절반 분량이다. 이러한 개인정보 유출 사건이 끊이지 않는 것에 대해 관련 전문가들은 각 기업들이 고객의 개인정보 수집엔 적극적이지만 이를 보호하는 DB보안에는 소홀하기 때문이라고 분석한다.[13][19]

2. DB 보안

DB 보안이란 관리 대상인 데이터베이스를 비 인가된 사용자로 부터 변경, 파괴, 정보 누출을 발생시키는 사건으로부터 보호하기 위한 방법을 말한다. DB 보안 방법은 크게 데이터베이스의 입출력 경로를 감시하는 접근제어 및 감사방식과 데이터베이스 내부의 데이터 자체를 암호화하는 암호화방식으로 구분된다.[15]

2.1 DB 보안 차원

DB 보안은 데이터베이스 보안 솔루션을 통해 관리해 온 것이 아니라 그림 1 처럼 단계적으로 데이터베이스를 보호하기 위한 일반적인 원칙을 기준으로 관리해 왔다. 이러한 데이터베이스 보안 일반원칙은 크게 다섯 가지로 구분된다. 첫째 네트워크차원의 보안, 둘째 시스템차원의 보안, 셋째 데이터 차원의 보안, 넷째 사용자관리차원의 보안, 다섯째 사용자 암호관리차원의 보안으로 구분된다.[5]

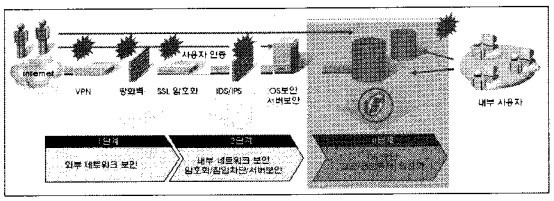

그림 1. 단계별 정보보호시스템의 구성
Fig 1. Configuration of protective information system by a step

2.2 DB 접근제어 및 감사

접근제어는 사용자 인증 및 권한을 강화하여 비인가자가 데이터베이스의 중요 테이블에 접근하여 데이터의 유출, 위·변조하는 행위를 차단하는 기술이다.[15]

접근제어 기술은 사용자 인증 및 권한을 네트워크의 TCP/IP기반으로 제어하여 비인가자의 불필요한 데이터 접근과 권한오용을 원천적으로 차단한다. 통제범위는 접근방식에 상관없이 테이블 및 특정 필드의 데이터를 포함하여 사용자가 실행하는 SQL질의어, 애플리케이션, OS커맨드 등까지도 통제 가능하다.

접근제어 기술의 원리는 모든 접근방식을 리모트 접근방식으로 처리 한다는 것이다. 즉 모든 사용자의 세션은 리스너 서비스를 통하여 데이터베이스에 접근하도록 강제하고 구현방식에 따라 패킷을 분석하여 사용자의 행위를 통제하는 것이다. 이러한 패킷분석과 차단행위는 데이터베이스 외부에서 수행되기 때문에 서버의 과부하나 성능저하를 최소화할 수 있는 장점과 더불어 사용자들이 수행한 작업내용 등을 감시하여 자체적으로 로그 기록을 할 수 있는 데이터베이스 보안기능이다.

접근제어 및 감사 솔루션 제품들은 그림 2와 같이 패킷분석 및 로그기록 방법에 따라 미러링 혹은 패킷 스니핑을 이용한 방식, 서버에 에이전트를 설치하는 방식, 게이트웨이 방식으로 구분된다.

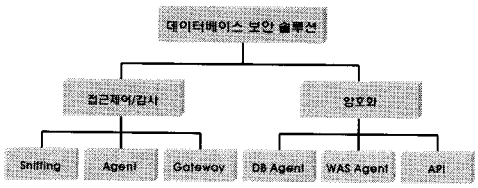

그림 2. 데이터베이스 보안 솔루션
Fig 2. Database security solution

2.3 DB 암호화

발생 가능성이 있는 데이터 유출에도 중요 정보의 악용을 막기 위해서는 데이터를 암호화하는 것이 가장 안전하고 확실하다. 그림 2에서 DB 암호화를 위해서 DB 서버에 에이전트를 설치하거나 데이터베이스 내부에 API를 설치하는 방식과 별도 서버에 암호화 에이전트를 설치하여 시스템의 과부하를 감소시키는 방식이 있다.[10]

2.4 DB Masking

데이터베이스 Masking은 DB 암호화와 유사한 방법으로 사용자가 의도적이거나 비의도적으로 데이터베이스에 접근하여 테이블 내의 중요 칼럼 또는 중요 내용을 참조할 경우 관리자에 의해 설정된 정책을 통하여 원본 데이터의 수정 없이 사용자로부터 데이터를 은닉하도록 하는 데이터베이스 보안 시스템이다. 데이터베이스의 질의 결과에서 주민번호(740730-1234567)가 있는 경우 리턴되는 데이터를 740730-******* 등과 같이 관리자가 의도한 형태로 데이터를 마스킹 처리하는 방법이다.[2]

3. DB 보안의 문제점 분석

DB 보안성 강화를 위한 연구로 접근제어 및 감사, 암호화 등 DB 보안 시스템별 취약점을 분석한다.

3.1 접근제어 및 감사 기술의 문제점

패킷분석 및 로그기록 방법에 따라 미러링 혹은 패킷 스니핑을 이용한 방식으로 서버에 에이전트를 설치하는 방식, 게이트웨이 방식으로 구분되며 이러한 구현 방식에 따라 해결해야 할 과제들이 있다.

■ 패킷 스니핑 방식

네트워크의 패킷정보만을 사용하여 정보를 수집함으로써 로그정보가 100% 확실하다는 보장이 없고 신뢰성이 부족하며, 특정 포트를 사용하는 소켓통신과 로컬 접근방식으로 수행되는 작업에 대해 사전통제 및 사후감사를 하지 못한다는 한계가 있다.

■ 에이전트 방식

정보에 대한 신뢰성은 가장 우수하지만 서버의 자원을 사용하기 때문에 대용량 트랜잭션 처리 시 서버의 성능을 급격히 감소시킬 뿐 아니라, 장애 시 이중화 구현이 불가능하여 보안의 무중단 대책이 사실상 어렵다.

■ 게이트웨이 방식

사용자의 모든 세션을 게이트웨이 장비를 거치도록 네트워크 구성이 되어야 하며, 중요 미들웨어나 애플리케이션 서버를 통해 접근하는 경우 IP별 통제가 사실상 불가능하다.

■ 공통적인 문제점

위의 DB 보안 방식이 가지고 있는 성능한계와 더불어 애플리케이션 서버 또는 데이터베이스 링크를 이용하여 우회적으로 접근하는 세션을 통제하기 어렵다. 또한 데이터베이스 불법유출 사고가 발생 했을 시 정보가 암호화 되어 있지 않은 경우에는 정보유출에 대한 대책이 사실상 없다.[20]

3.2 암호화 기술의 문제점

데이터 암호화는 DB 보안을 강화할 수 있는 필요한 기술이지만, 이를 적용함으로 인하여 아래와 같이 6가지 예상치

못한 부작용과 역효과가 발생할 수 있다.

■ 인덱스 색인 검색의 제약

데이터암호화에 있어서 테이블과 더불어 인덱스도 암호화의 대상이다. 테이블의 중요 데이터만 암호화하는 것은 보안의 효용성이 저하되며 데이터 유출 및 악용의 위험성이 여전히 존재할 수밖에 없다. 인덱스 암호화로 인한 데이터 정렬체계 훼손으로 DB성능저하의 직접적인 원인이 된다.

■ 객체관리 혼란 및 사용 제약

View와 Trigger의 사용으로 실제 데이터 객체와 접근객체가 상이하고, 예상치 못한 제약사항으로 인하여 일부 애플리케이션의 수정이 필요하거나 유틸리티 사용불가 등의 부작용이 발생하기도 한다.

■ 심각한 DB 성능 저하

DB 암호화를 위한 Encryption/Decryption 알고리즘 수행으로 Overhead가 발생하고 Table Full Scan으로 인해 암호화된 인덱스의 데이터 검색속도가 저하될 뿐 아니라 배치처리, 부분범위 처리 시 급격한 처리속도가 발생한다.

■ 실시간 데이터 암호화 미지원

DB 암호화 대부분의 솔루션들이 실시간 데이터 암호화가 불가하고, 대용량 테이블의 암호화 적용 시 장시간이 소요되어 서비스가 중단될 수도 있다. 또한 암/복호화 데이터 저장에 따른 스토리지 용량도 증가되고, 암호화 적용 시 DML이 수행되므로 noArchive Mode 운영을 고려하여야 한다.

■ IP기반의 데이터 접근통제 미지원

암호화된 컬럼은 사용자 계정별로 액세스 차단, null, 치환값으로 접근제어를 하여야 하고, 네트워크 IP기반으로는 접근제어가 불가하여 사용자 계정을 공유하는 환경에서는 실효성이 없다. 그러므로 접근제어 및 감사기능을 병행하여 불법 데이터 유출을 차단해야 한다.

■ 추가적인 문제점

현재 개발된 기술별로 차이가 있으나 LONG, LOB 데이터 형태 등의 암호화 적용이 불가하고, Null값 데이터의 암호화 적용이 불가하고, LONG데이터가 있는 테이블은 모든 컬럼에 암호화가 불가하고, 암호화된 테이블의 컬럼 추가 시 복호화 후 재 암호화해야 하는 제약사항이 발생하며, 암호화된 테이블의 DB속성이 유실될 수 있고, 암호화 적용으로 SQL Script 및 애플리케이션 수정 사항이 발생할 수도 있다.[9]

4. Masking 기술의 문제점

DBMS의 기밀성과 가용성을 확보하기 위해 DB Masking 기술의 문제점을 분석한다.

4.1 기존 기술의 문제점

DB Masking 기술의 문제점은 아래와 같은 6가지 이유로 조직의 정책과 사용자의 선택에 제약이 따르며 업무 및 관리 차원의 어려움이 발생할 수도 있다.

- 특정 DBMS version에서의 자체 기능만으로 제공이 되고 있으며, 범용 적이지 못하다.(각각의 데이터베이스별로 설정해야 하거나 아예 기능이 없는 DBMS도 있음)
- 특정 테이블의 컬럼에 대해 보호를 하기 위해서 별도의 보호하고자 하는 컬럼이 없는 뷰 테이블을 생성하여야 하는 별도의 작업을 필요로 한다.
- 특정 칼럼의 내용을 보호하기 위하여 사용자는 지원되는 한 가지의 전용 응용 프로그램만 사용 가능하다.
- 데이터베이스의 특정 유형의 데이터 보호를 위하여 지정 응용프로그램을 사용하지 않으면 사용자 제어 불가 또는 DBMS 사용 불가하다.
- DBMS사용 시 업무 효율을 위하여 사용자는 다양한 응용프로그램을 사용하고자 하지만 제약이 발생한다.
- 전용 응용 프로그램 사용 시 관리자에 의한 정책을 설정, 배포상의 번거로움 및 중앙 관리의 어려움이 발생한다.

4.2 DBMS의 뷰 테이블 이용 시

기존 구성 방법 중 뷰 테이블을 이용한 방법의 처리절차 그림 3과 같다.

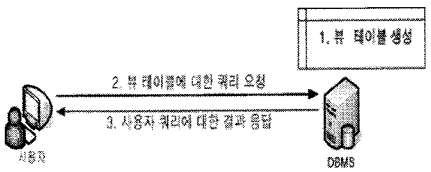

그림 3. DBMS 뷰 테이블 이용
Fig 3. DBMS View table use

[1] 사용자에게 특정 칼럼만 보여지기 위하여 뷰 테이블을 생성한다. [2] 사용자는 DBMS에 접속하여 처리하고자 하는 뷰 테이블에 접근하기 위해 쿼리를 전송한다. [3] DBMS는 요청 받은 쿼리에 대한 처리를 하여 결과값을 사용자에게 전송한다.

그림 3과 같이 많은 수의 테이블 조인을 통한 뷰 테이블의 빈번한 생성은 시스템의 성능 저하를 일으킬 수 있으며, 보안과 관리의 측면에서 중요한 정보에 대한 세부적인 접근에 대한 제어 및 모니터링을 처리 할 수 없다.

4.3 사용자 전용 프로그램 이용 시

기존 구성 방법 중 사용자 전용 프로그램을 이용한 방법의 처리절차 그림 4와 같다.

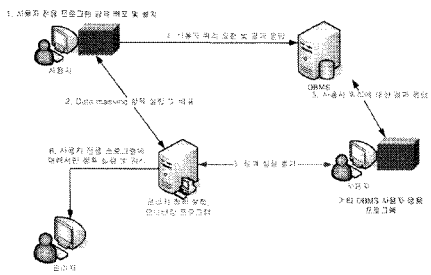

그림 4. 사용자 전용 프로그램 이용
Fig 4. Program use only a user

1 데이터 마스킹 정책에 의해 중요 데이터를 사용자로부터 보호하기 위하여 사용자 전용 프로그램을 사용자 PC에 강제 배포 및 설치를 하도록 해야 한다. 2 사용자에게 설치된 데이터 보호 기능의 전용 응용 프로그램은 관리 서버로부터 데이터 마스킹 정책을 받아서 보관한다. 3 이 때 사용자 전용 프로그램이 설치되지 않은 응용 프로그램은 데이터 마스킹 정책을 받지 못한다. 4 사용자 전용 프로그램에 의해 쿼리를 수행하고 해당 결과를 수신한다. 그리고 사용자 전용 프로그램에 의해 데이터 마스킹 처리가 이루어진다. 5 기타 DBMS 사용자 응용 프로그램에 대해 수행된 중요 데이터 결과는 그대로 사용자에게 전달되어진다. 6 사용자 전용 프로그램에 대해서만 정책 설정 및 감시가 가능하며, 기타 DBMS 사용자 응용 프로그램에 의한 사용자는 감시를 할 수 없다.

그림 4와 같이 사용자는 DB 마스킹 기능을 포함하고 있는 특정 프로그램만을 사용하여야 하는 제약이 있고, DB 마스킹 정책을 도입하기 위해 사용자 전용 프로그램 도입, 설치, 운용 등이 필요하므로 물리적, 시간적인 추가 비용이 소요된다. 또한 사용자가 특정 프로그램 이외의 것을 사용 시 사용자의 제어가 불가능하다는 문제점이 있다.[20]

III. 보안등급별 DB Masking 연구

DB 보안을 위한 종합적인 보안 프레임워크의 제안과 보안등급별 DB Masking 방법을 제안하고, 만약의 침해사고에 대비한 감사기록 수집에 관해 연구한다.

1. DB 보안 가이드라인

DB 보안을 위한 중요정보의 유출 방지를 위해서는 무엇보다 기업과 국가 차원에서 사람에 대한 보안교육으로부터 시작하여야 한다. 다음 절차로 그림 5와 같이 보호하고자 하는 최종 목적지인 DB를 보안하기 위해서는 기본적으로 접근 가능한 주변 환경들을 통제하고 접근 권한이 있는 사용자들을 세분화해서 관리해야 한다. 이와 더불어 DB보안 솔루션을 더 유용하게 사용하기 위해서는 범용적인 DBMS 통합관리, 패턴 매칭, 이중화, Telnet/FTP 통제, DB부하 감소, 사전/사후 결재 및 무결성 체크, 불법 접근 시 경보(이메일, SMS 등), 세션관리 등 추가적인 확장 기능을 통해 DB 보안의 실용도를 높일 수 있다.

■ DB 접속 경로 설정

접근 및 권한제어의 기능을 향상시키기 위해서 데이터베이스를 사용하는 보안 적용 대상자들은 DB보안 솔루션을 통해 접속해야 하고, 정책설정을 위해서는 기관이나 기업의 상황에 맞게 체계적으로 그룹을 분리시킨다.

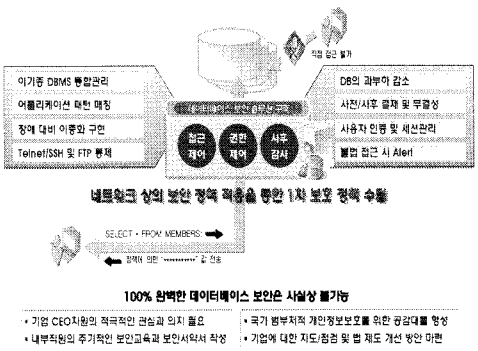

그림 5. 종합적인 DB 보안 프레임워크
Fig 5. Comprehensive DB security framework

■ 여러 종류의 DBMS 통합 관리

하나의 DB보안 솔루션을 통해 Oracle, MSSQL, Sybase, Informix, DB2, TeraDB, Altibase 등 여러 유형의 DBMS를 통합 관리(서비스, 정책설정 및 로깅, 리포팅)한다.

■ 애플리케이션 패턴 매칭

DBMS Application의 Pattern을 기억하여 사용자가 임의적으로 Application을 변조하여 접속하여도 접속 Pattern을 통하여 사용하는 Application을 확인한다.

■ 장애 대비 이중화 구현

DB보안 솔루션의 장애를 대비해서 L4 스위치 등을 통해 이중화로 구성한다. 지속적인 데이터베이스 보안을 위해서는 Fail Over와 같은 기능도 사실상 구현해서는 안 된다. DB보안 솔루션이 장애가 발생하였다고 서비스를 위해 Bypass하는 것은 보안상 결함을 낳게 되기 때문이다. DB보안 솔루션의 이중화 구성은 한쪽 시스템의 장애에도 데이터베이스 보안의 연속성을 유지할 수 있다.

■ Telnet/SSH 및 FTP 통제

DBMS가 운영되는 운영체제(UNIX)상에 접속하여 실행시키는 모든 행위를 통제 및 모니터링하기 위해 Telnet/SSH와 FTP 서비스에 대해서도 DBMS와 동일하게 모니터링 및 접근제어를 수행한다.

■ DB의 과부하 감소

명령어 실행에 대한 권한 제어 통제 뿐 아니라 그 명령어로 인한 DB의 부하를 증가시키는 행위에 대해서 제어한다. 지정된 시간이 지나도록 DB 서버에서 사용자에게 요청 값을 통보하지 못할 시에는 해당 사용자의 세션을 강제로 kill 시킴으로써 DB 서버의 과부하를 줄인다.

2. 범용적인 Masking 기술 연구

제조사 기술에 한정된 Masking 기술을 Gateway 서버 형태의 범용적인 Masking 기술로 발전시켜 DBMS의 종류에 관계없이 모든 종류의 DBMS에 대해서 동일한 통제정책으로 DB의 질의 결과 값을 데이터 마스킹이 가능하도록 한다.

만약에 DB 정보가 유출되었을 시는 이를 활용하지 못하도록 DB 마스킹 처리 하여야 하는데, 마스킹 처리의 기준은 사용자별 보안 등급을 통해 설정하고, 개개인별로 가상계정을 통해 접속하도록 하는 방법을 새로 제안한다.

위와 같은 Gateway 서버 형태의 Masking 기술은 DB서버와 별도로 운영되며 SQL 쿼리에 대한 트래픽만을 소화하기 때문에 속도에 대한 문제도 동시에 해결할 수 있다.

2.1 Masking 서버 접근 통제

접근 및 권한제어의 기능을 향상시키기 위해서는 그림 6과 같이 데이터베이스를 사용하는 보안 적용 대상자들은 DB보안 솔루션을 통해 접속해야 하고, 정책설정을 위해서는 기관이나 기업의 상황에 맞게 체계적으로 그룹을 분리시켜야 한다.

DB보안 솔루션을 통해 접속하게 하는 방법은 세 가지가 있다. 첫 번째로 ACL(Access Control List)은 특정 네트워크의 불필요한 트래픽을 줄이거나 사용하지 않는 특정 서비스 등의 사용 방지를 하기 위한 방법이다. ACL 기능을 이용하여 DB로 접근하는 사용자에 관한 리스트를 지정하고 지정한 네트워크 설정을 통하여 DB보안 솔루션을 통하지 않는 경로를 차단할 수 있다. 두 번째로 방화벽의 정책을 통하여 접근을 통제 하는 설정을 할 수 있으며, 마지막으로는 DBMS 파일을 수정하여 특정 IP나 IP대역의 접근만을 허용하는 방법으로 접근을 통제하는 방법이 있다.

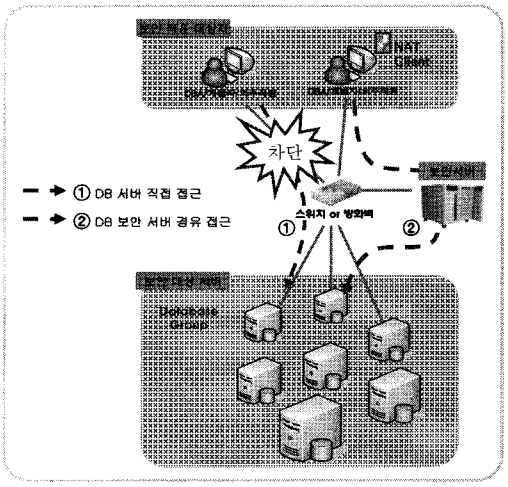

그림 6. DB보안을 위한 접근 통제
Fig 6. Access control for DB security

2.2 범용적인 DB Masking 방법

이기종 DB의 통합적인 보안 정책 설정을 위해 그림 7에서 업무 흐름 순서대로 각 부문의 역할을 체계적으로 도식화 하였으며, 다음과 같이 6단계로 업무를 수행한다.

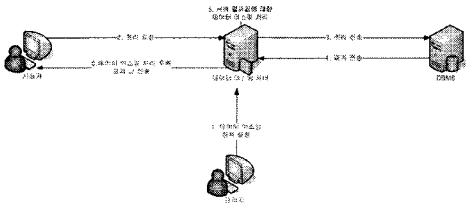

그림 7. DB 마스킹 업무 흐름도
Fig 7. DB masking working flow chart

[1] 관리자는 DB 마스킹 서버에 사용자로부터 중요 데이터 보호를 위해 정책 설정을 한다. [2] 사용자는 DB 마스킹 서버를 통해 DBMS로 쿼리를 요청한다. [3] DB 마스킹 서버는 사용자 쿼리를 DBMS 서버에 전송한다. [4] DBMS 서버는 그에 대한 결과를 데이터 마스킹 서버에 전송한다. [5] DB 마스킹 서버는 DB 마스킹 정책에 설정된 것을 서버 응답 값과 비교하여 DB 마스킹이 필요한 경우 해당 데이터를 특수 문자(예: '*' (asterisk))로 마스킹 처리한다. [6] DB 마스킹 처리된 결과 값이 사용자에게 전달되고, 사용자는 서버 응답 값 중 일부 데이터가 마스킹 처리된 결과 값을 수신한다.

2.3 DB Masking 기술 적용 방식

DB 마스킹 기술은 그림 8과 같이 7단계로 진행된다. 정규식 표현을 설정하여 서버 응답 문자열 값 중 해당 정규식 표

현과 일치하는 경우에 문자열을 마스킹 처리하는 정규식 표현에 의한 DB 마스킹 기법과 관리자에 의해 지정된 테이블 및 컬럼에 대해 데이터를 마스킹 처리하는 테이블 및 컬럼 지정에 의한 DB 마스킹 기법이 있다.

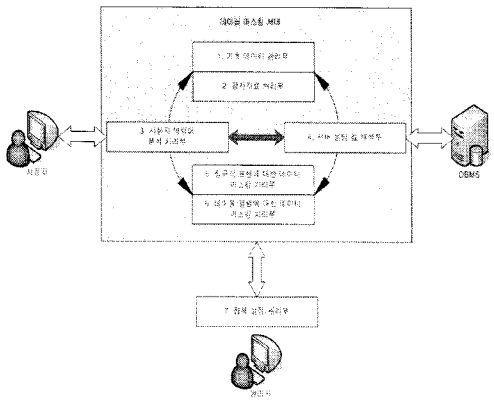

그림 8. DB Masking 적용 순서
Fig 8. DB Masking application order

1 DB 마스킹 시스템에서 사용되는 전체적인 기초자료는 모두 서버에서 관리한다. 기초 자료는 정규식 표현 정보, 테이블/컬럼 지정 정보, 관리 대상 DBMS 정보, 데이터 마스킹 정책, 감사자료 기록 정책 등이 있다. 2 사용자 명령어와 DBMS의 결과 데이터는 분석되어 기초 데이터상의 감사자료 정책에 의하여 기록한다. 3 사용자는 DB 마스킹 서버를 통해 DBMS로 사용자 명령어를 요청하게 되는데 이 때 DB 마스킹 서버에서는 제일 먼저 사용자 명령어의 형태와 기본 정보를 추출하여 분석 한다. 4 분석된 데이터와 기초 자료의 DB 마스킹 정책을 근거로 DB 마스킹을 수행 대상인 테이블, 컬럼 및 행 정보를 해석 및 추출한다. 5 추출된 데이터 결재 대상인 테이블, 컬럼 및 행 정보를 설정된 정규식 표현에 대한 DB 마스킹 정책에 의해 부합되는지 분석한다. 정책에 부합되는 경우 정보를 마스킹 처리한다. 6 추출된 데이터 결재 대상인 테이블, 컬럼 및 행 정보를 설정된 테이블/컬럼에 대한 DB 마스킹 정책에 의해 부합되는지 분석한다. 정책에 부합되는 경우 정보를 지정된 컬럼에 대해 마스킹 처리한다. 7 관리자에 의해 정규식 표현, 테이블/컬럼 지정에 대한 DB 마스킹 정책을 설정 및 관리할 수 있도록 한다.

3. 가상계정을 이용한 제어 및 사고 처리

우리나라 DBMS 관리 현황을 보면 동일한 계정을 사용함으로써 누가 행위자인지 정확히 알아내기가 어렵다. 이러한 문제를 해결하기 위해 사용자의 가상계정을 이용하여 DB를 사용하게 하고, 접속 로그를 감사(Auditing)자료로 생성하게 하여, 사고 처리에 대비한다.

3.1 가상계정을 통한 사용자 인증

NAT Agent를 통해 1인 1계정(가상계정)을 등록하여 DB서버 접근 시 등록한 아이디/패스워드로 로그인하도록 한다. 사용하여 누가, 언제, 어떠한 행위를 했는지 저장 하여 더욱 강력하고 편리한 DB보안을 시행한다. 또한 기 등록된 가상계정 사용자를 보안등급별로 분류하여 Masking처리된 정보와 Masking이 해지된 정보를 구분하여 제공하도록 설정하고, Masking이 해지되어 정보가 제공 되어지는 권한자들에 대해서는 보다 엄격한 보안교육 및 서약서를 통해 보안사고를 사전에 예방하는 효과를 거둘 수 있다.

3.2 SQL문 사전/사후 결재 및 무결성 체크

각 DB 서버를 그룹별로 나누고 그룹에 대한 권한을 부여받은 관리자는 사용자가 요청한 SQL문에 대하여 검색과 결재를 통해 승인한다. 결재가 필요한 SQL문은 결재가 승인될 때까지 기다리게 되며, 보안 등급이 낮아 승인 받지 않고 DB를 미리 처리하는 경우에도 설정을 통하여 사후 결재처리하거나, 로그 기록으로 남기도록 한다. 또한 기존의 Workflow와 연동하여 결재 전·후 데이터 보관, 작업요청 및 결재 이력을 보관하여 사고 처리에 대비한다.

4. DB 보안 문제점과 개선안

본 논문에서 분석한 DB보안의 문제점과 문제점의 개선을 위한 제안 사항을 표 1에 정리 하였다. DBMS와 DB 보안 분야에 전문가로서 본 논문에서 제안한 내용은 DB 보안의 문제점으로 분석된 내용들을 확실하게 해소 할 수 있는 방안으로 효과를 나타나게 될 것이다.

표 1. DB 보안 문제점과 개선안
Table 1. DB security problem and improvement data

DB 보안 문제점	논문에서 제안한 개선점
접근제어, 감시 문제점 - 패킷 스니핑 방식 - 에이전트 방식 - 게이트웨이 방식	가상계정 사용 제안 - 가상계정을 통한 사용자 인증 - SQL문 사전/사후 결재 및 감사기록 무결성 체크
암호화 기술 문제점 - 인덱스 검색 제약 - 객체관리 혼란 및 사용 제약 - 심각한 DB 성능 저하 - 실시간 데이터 암호화 미지원 - IP기반의 데이터 접근제어	DB Masking 기술 제안 - DB 마스킹 모두 서버에서 관리 - DBMS의 결과 감사자료 기록 - 사용자 형태와 정보 추출 분석 - 마스킹 정책에 의해 부합 분석 - 정책 부합 정보 마스킹 처리

미지원	- 결재 대상 마스킹 정책분석 - 마스킹 정책을 설정 및 관리
Masking 기술 취약점 - DBMS의 뷰 테이블 이용 문제 - 사용자 전용 프로그램 이용 문제	범용적인 DB Masking 제안 - 관리자 DB 마스킹 정책 설정 - 사용자는 DBMS로 쿼리 요청 - DBMS 서버에 전송 - 결과 DB 마스킹 서버에 전송 - DB 마스킹 정책과 비교 - 특수 문자 '*' 마스킹 처리 - 마스킹 처리 결과 값 수신

IV. 결 론

DB 보안을 위해 암호화 모듈을 실행시키면 성능이 저하되어 실무적으로 사용이 미미한 실정이다. DB 보안에 대한 암호화만을 고집하는 것은 실무적인 사용자의 입장을 고려하지 않는 것이다.

본 논문에서는 DB에 대한 성능의 저하를 가져오는 보안의 인덱스검색, 객체관리 혼란, 암호화로 인한 심각한 DB 성능 저하, 실시간 데이터 암호화 미지원, IP기반의 데이터 접근통제 미지원으로 인한 기술별로 DB 보안의 문제점을 분석한다.

그리고 DB 보안을 유지하면서도 가용성을 향상시키기 위해 암호화기술의 대체수단인 DB Masking 기법을 활용한 종합적인 보안 프레임워크를 제시한다. 또한 논문에서 제시한 개선안으로는 가상계정을 이용하여 보안등급별로 DB Masking 기준을 설정하고, 가상계정을 통한 사용자 인증과 SQL문의 사전과 사후 결재 및 무결성을 체크하고, 감사로그로 수집하여 DB를 안전하게 관리 할 수 있는 방안을 마련한다. 감사기록은 가상계정을 통한 사용자 인증을 통해 로그인 정보와 접근경로 등의 로그 정보를 저장하고, 사용자의 행위에 대한 사전/사후 데이터 비교를 통해 무결성을 입증시킨다.

본 논문에서 제안한 방법은 실무적인 차원에서 DB보안이 이루어지면서, 실제적인 성능의 저하를 가져 오지 않는 개선안이 될 것이며, 제안한 데이터 마스킹 기법은 사용자와 DBMS서버에 별도의 프로그램 설치나 설정 변경이 필요 없어 호환성을 가지고, 뛰어난 가용성을 확보할 수 있다.

중앙 집중 방식인 본 데이터 마스킹 기법은 보안등급별 권한제어, 관련 정보(로그, 감사기록 등) 취합, 업무 처리 및 관리 방법이 향상될 뿐만 아니라, 기존의 데이터 마스킹 기법과 같이 전용 클라이언트가 있어야지만 동작하는 것과는 무관하게 비전용 클라이언트 툴 사용 시에도 데이터 마스킹에 의해 중요 데이터 보호가 가능하다.

향후 연구 목표는 Encryption/Decryption 시 발생하는 속도에 대한 문제를 해결할 수 있는 알고리즘 연구하여 Masking 방법 보다 높은 보안성을 확보하고, 3Tier로 접근하는 사용자에 대한 세분화된 접근/권한 제어 및 감사기록 저장을 통해 우회 경로를 통한 침해에도 적극적으로 대처할 수 있는 인공지능형 보안 감사 기술을 연구가 필요하다.

참고문헌

[1] 정보통신부, *정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(전부개정 2008. 2. 29, 대통령령 제20668호)*, 2008년 2월.

[2] 교육과학기술부, "*교육과학기술부 및 교육·연구기관의 개인정보관리 업무편람*," 85쪽, 2008년 5월.

[3] 정보통신부, *개인정보보호지침고시 및 개인정보보호 핸드북*, 2005년 7월.

[4] 국제협력개발기구(OECD), *개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인(GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANS BORDER FLOWS OF PERSONAL DATA)*, 1980년 9월.

[5] 노시춘, "데이타베이스 보안과 Oracle 보안 구현방법," 남서울대학교, 2005년 11월.

[6] 김정상, "개인정보 침해사례를 통한 데이터베이스 보안에 관한 연구," 건국대 정보통신대학원, 2007년 6월.

[7] 이강석, "데이터베이스 사용자 사전 통제 및 사후 추적을 통한 데이터베이스 보안 연구," 한양대 공학대학원, 2007년 2월.

[8] 행정안전부, "개인정보 다량취급 업체 관리감독 강화," 정보보호 21c, 2008년 10월.

[9] 금융결제원, "DB보안 기술의 현황과 문제점 분석," Information Security Conference 2007, 2007년 9월.

[10] 한국전자통신연구원, "데이터베이스 암호화 기술과 제품 동향," 전자통신동향분석, 제 22권, 제 1호, 105-113쪽, 2007년 2월.

[11] 옥션, "*회원정보 유출됐다*," 한겨레 신문, 2008년 2월.

[12] GS칼텍스, "*1천만명 정보유출*," 연합뉴스, 2008년 9월..

[13] 국정감사 박상돈 국회의원, "*개인정보 유출, 전 국민의 절반이 당했다*," 뉴시스, 2008년 10월.

[14] DatabaseSecurity(Common-sensePrinciples). *http://www.governmentsecurity.org/articles/DatabaseSecurityCommon-sensePrinciples.php*

[15] 문형진, "역할기반 접근제어시스템에 적용가능한 민감한 개인정보 보호모델," 한국컴퓨터정보학회논문지, 제13권 제5호, 103-110쪽, 2008년 9월.

[16] Qiang Lin. Ph.D. Defense In-Depth to Achieve, "Unbreakable," Database Security, 2004.

[17] Kevin Kenan, "*Cryptography in the Database-The Last Line of Defense*," Addison-Wesley, Oct. 2005.

[18] Rich Mogull, "Database Activity Monitoring Is a Viable Stopgap to Database Encryption for the Payment Card Industry Data Security Standard (and Beyond)," Gartner, July 2006.

[19] 박대우, "모바일 포렌식 자료의 추출과 무결성 입증 연구," 한국컴퓨터정보학회논문지, 제12권 제6호 177-185쪽, 2007년 12월.

[20] 백종일, "*데이터베이스 보안을 위한 가용성 확장 연구*," 숭실대학교 정보과학대학원, 2008년 12월.

[21] Dea-Woo Park, "A Study on Problem of Korean-Digital Forensic," International Conference on Ubiquitous Information Technologies & Application, ICUT (1976-0035), Dec. 2008.

저 자 소 개

백 종 일

2005년 8월: 한국방송통신대학교 미디어영상학과 (공학사)
2009년 2월: 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
2009년 4월: 호서대학교 벤처전문재학원 IT응용기술학과 (박사재학)
2005년 9월 ~ 현재: (주)조은아이앤에스 정보보안팀 팀장
〈관심분야〉 DataBase 보안, 정보보호, DB 포렌식, 정보보호 시스템, 유비쿼터스 보안 등

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence