통합 DB의 취약점 분석 및 제어 연구

백종일*, 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study on Analysis and Control by Vulnerability of Integrated Database

Jong-Il Baek*, Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

e-mail: jibaig101@empal.com, prof1@paran.com

요 약

현재 DB 보안시스템에서 DB 서버의 주요정보 및 개인정보 등의 전체 오브젝트 정보를 파악하여 보안취약 오브젝트에 대한 인지 및 차단을 수행하고, 업무범위를 벗어난 접근 등에 대한 오남용을 방지하고, 보안취약점을 자체 점검해야 할 필요성이 있다. 본 논문에서는 현 기술로 제어 불가한 DB의 보안취약 오브젝트에 대한 추출과, 추출 정보의 저장 및 관리, 메모리에 적재 및 오브젝트 명과 정보의 치환 분석 등의 보안 적용방안을 연구한다. 또한 보안 대상 내 주요 오브젝트의 변경이력을 관리하고, 보안 취약 오브젝트의 스캔결과 및 정책의 기본관리, 예약수행관리, 관리자 통보 등의 관리방안을 연구한다. 보안 취약에 대한 사전 차단을 위한 제어가능 시스템과의 연동은 ESM 등 정보수집 모듈과의 연동 및 보안정책 적용결과에 대한 연동 및 정책 재적용 방안을 설계한다. 본 논문의 연구는 지능형 DB보안 기능구현을 가능케 할 자료로 사용될 것이다.

키워드

DB보안(DB Security), 취약점(Vulnerability), 데이터마이닝(Data Mining)

Ⅰ. 서 론

일본은 2005년 4월 개인정보보호법을 시행하여, 5천명을 초과하는 개인정보를 보유한 기업은 개인정보 부정취득과 유출을 방지해야 하고, 이를 어길 경우 6개월 이하 징역 또는 30만 엔 이하의 벌금을 부과하고 있다. 일본의 이와 같은 움직임은 단순히 개인정보보호법 때문이라기보다 금전적인 피해와 기업 이미지의 손상, 나아가 기업의 생존여부를 결정할 수 있다는 위협에 대해 기업들이 인식하기 때문이다.

안전한 정보보호 프레임워크 구축을 하여 IT839 전략의 일환으로 추진되는 융합보안프레임워크(FSF, Fusion Security Framework, 融合保安)에서 추구하는 안전한 인터넷(Secure Internet), 깨끗한 인터넷(Clean Internet), 프라이버시가 보호되는 인터넷(Privacy-guaranteed Internet)에 관련한 개인정보보호의 요구도 또한 증가 하고 있다. 이에 따라 각기 다른 정보보안 기능을 가진 보안 제품이 시스템적으로 협업할 수 있도록 구성되어 단일목적에서 다양한 목적으로, 독자적 보안에서 상호호환 형태로, 수동적 보안에서 능동적 보안으로 변화하고 있다. 중소기업의 중요 정보에 대한 보안에 있어서도 기존에 수동적이며 단순한 보안의 형태에서 지능적으로 보안 위협을 인지하여 관련 시스템과의 연동에 의한 능동적인 정보보안을 필요로 한다.

기업과 조직의 중요정보를 취급하는 DB서버와 보안시스템에서 DB 서버의 주요정보 및 개인정보 등의 전체 오브젝트 정보를 파악하여 보안취약 오브젝트에 대한 인지 및 차단을 수행하여서, 업무범위를 벗어난 접근 등에 대한 보안 오남용을 방지하고, 보안취약점을 자체 점검해야 할 필요성과 이를 체계적으로 연구하여 DB보안시스템을 강화할 필요가 있다.

본 논문은 Ⅰ장, 서론에서 논문의 필요성을 설명하고, II장, 관련연구에서는 DB보안 시스템의 국내·외 기술동향 및 기존시스템의 한계를 정리한다. III장에서는 통합 DB의 보안취약 오브젝트 분석 및 제어방안을 제시하고, IV장에서 결론과 향후 연구를 설명한다.

II. 서 론

2.1 기존 DB보안 시스템의 구현 방식

2.1.1 국내 기술 동향

국내에는 DB 서버에서 수행되는 보안취약 오브젝트에 대한 보안위배 탐지 및 제어 기능 등을 제공하는 지능형 보안분석 솔루션은 존재하지 않으며, 서버 취약점 점검 툴은 일부 제품이 있다. 그리고, 게이트웨이 방식과 스니핑 방식의 접근제어와 감사기능 만을 하는 DB보안시스템이 있으며 다음과 같다[6].

■ 제조사/제품명 : ㈜웨어벨리/샤크라

특징: 스니핑 방식을 주력으로 하는 DB보안 시스템으로 중앙 관리 서버를 통해 사용자의 DBMS 접속에 대해 모니터링 및 감사 로깅 기능을 수행한다.

■ 제조사/제품명 : ㈜소만사/DB-i

특징: 게이트웨이 방식와 스니핑 방식을 제공하는 접근제어 방식의 DB보안 시스템으로 게이트웨이방식에서 이중화 기능을 지원하며 중앙 관리 서버를 통해 모니터링 및 감사 로깅 기능을 수행한다.

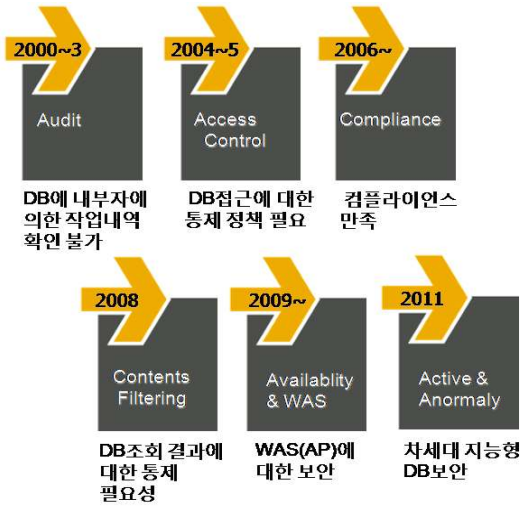

그림 1. DB보안 이슈의 변화

최초의 DB보안은 감사데이터 생성을 목적으로 sniffing 형태의 제품이 개발되어 유용하게 사용되기는 하였으나 100% 로깅이 불가하다는 한계점이 있다[4]. 2000년대 중반부터 gateway 방식의 DB접근통제 시스템은 Loss가 없다는 장점뿐만 아니라 DB보안에 필요한 정책을 부여해 보안을 한층 강화시키는 방법이다[5]. 이후 불특정 다수의 DB조회 결과에 대한 통제의 필요성이 대두되어 중요정보에 대해서는 Data masking 기술을 통해 유출을 방지하도록 설계하였다. 최근의 DBMS 보안 이슈는 그림 1과 같이 차세대 지능형 DB보안 시스템을 필요로 하고 있으며, 현재 기술로는 한계에 봉착되어 있다[2].

2.1.2 국외 기술 동향

해외의 유명 제품들 중 네트워크상에서 수행하는 접근제어 형태의 DB보안 기능을 수행하는 제품은 아래와 같으며 지능형 보안 분석 솔루션은 존재하지 않는다.

■ 제조사/제품명 : 가디움/SQL Guard

특징: 접근제어 방식의 DB보안 시스템으로 중앙 관리 서버를 통해 사용자의 DBMS 접속에 대해 모니터링 및 감사 로깅 기능 및 전용 프로그램을 이용한 C/S기반의 데이터 마스킹 기능을 수행한다.

■ 제조사/제품명 : 인그리안/DataSecure

특징: 데이터 마스킹 기술을 이용하여 필드의 일부를 마스킹 처리할 수 있다. 특정 DBMS(Sybase ASE, MSSQL)에 대해서만 가능하며, DB 접속 툴 자체의 다양한 기능을 사용할 수 없다.

2.2 기존 DB보안 시스템의 한계

주요 정보에 대한 보안 솔루션인 DB보안 솔루션의 경우 다음과 같은 한계가 있다. 첫째, 서버 내에서 수행되는 보안취약 오브젝트에 대한 인지 및 차단이 불가하다. 둘째, 보안 정책상의 권한은 있으나 관련 업무의 범위를 벗어난 접근 등의 오남용 인식이 불가하다. 셋째, 시스템 내의 주요정보 또는 개인정보를 포함한 전체 오브젝트 정보의 파악이 불가하다. 넷째, DB 자체가 가지는 보안취약점에 대한 자체 점검 방안이 없다. 다섯째, 운영상 변경되는 오브젝트들에 대한 전반적인 변경이력 및 비교이력의 확인이 불가하다. 위와 같은 기존 DB보안 시스템의 한계를 극복하기 위해서는 DB의 보안취약 오브젝트에 대한 보안적용 기술 개발, DB 자체적으로 보유한 보안 취약성의 분석기술 개발, 지능형 프로파일링 기법을 이용한 변칙접근의 제어 기술 개발, 사전 차단을 위한 제어가능 시스템과의 연동 기술 개발 등을 필요로 한다[3].

Ⅲ. 통합 DB의 취약점 분석 및 제어

3.1 정보검색 및 추출을 위한 DB 통합 방안

3.1.1 정형/비정형 데이터의 통합 데이터 관리

정형 데이터뿐만 아니라, 비정형 데이터(이미지, 오디오, 비디오, 매핑데이터, 문서 등)를 기존 SQL문을 확장해 모든 데이터 유형을 통합DB로 처리한다.

■ XML DB 엔진 : 데이터 교환 및 문서 표준의 XML 문서를 관계형 데이터와 함께 통합DB에서 SQL, SQL/XML, XQuery 등으로 처리하고, XML Schema, XPath, XML Index를 처리하며, XML과 관계형 데이터간도 상호 변환을 지원한다.

■ SecureFiles : 기존에 지원했던 비정형, 대용량 데이터 타입인 LOB에 대해 고성능, 보안, 압축, 중복 제거 기능을 지원한다.

3.1.2 대용량 데이터 분할 처리 및 정보주기관리
Partitioning기능을 통해 하나의 Table 혹은 Index를 Partition이라는 더 작은 단위로 나누어 관리하는 방법으로 다양한 Partition 기법과 더 편리한 관리 방법을 제공하며 테이블, 인덱스의 장애 관리도 빠르게 대응한다.

3.1.3 데이터 압축 처리
데이터의 압축 저장기능으로 Storage 공간을 절약하고 OLTP 업무와 같은 Transaction 에서도 데이터 압축 처리로 성능 개선, 비정형데이터의 압축 및 중복제거로 리소스를 절감한다.

3.1.4 데이터 마이닝
통합DB 내에서 데이터마이닝을 통한 DB품질, 분석, 추론을 수행하며, 데이터마이닝 모델을 DB 객체와 유사하게 관리한다[7].
이와 같이 통합, 압축, 중복제거, 분석, 추론 등을 통해 보안취약 오브젝트 검색 및 추출 정보의 품질을 높인다.

3.2 취약점 분석 및 제어 방안
3.2.1 DB의 취약점에 대한 보안적용 방안
보안취약 오브젝트를 추출 하여 이를 저장 및 관리한다. 보안기능을 수행하기 위하여 저장 정보를 메모리에 적재하고 분석 시 오브젝트 명과 실 정보의 치환하여 처리한다.

3.2.2 DB 자체적으로 보유한 보안 취약점 분석방안
보안 취약성 정보 수집하여 이를 DB화하여 정보 제공을 위한 사용자 인터페이스를 지원한다. DB의 보안 취약성별 분석 기술을 설계하여 각각을 모듈화 하여 최종 통합한다.

3.2.3 지능형 프로파일링 기법을 이용한 변칙접근의 제어방안
DB 사용이력을 지정 시간마다 프로파일링 기법 적용하여 분석된 결과를 보관한다. 각 형태별로는 업무유형별, 주요접근유형별, 주요정보 또는 개인정보 유형별, 사용자 정의 유형별로 정보 수집 및 분석 알고리즘을 설계한다. 분석 정보를 이용해서 정책화 하는 기술을 개발하여 보안기능을 수행하도록 한다[1].

3.2.4 사전 차단을 위한 제어가능 시스템과의 연동
DB보안 시스템과의 밀착된 연동을 위한 프로토콜을 설계 한다. 프로토콜에 의해 연동된 보안 솔루션에서 정책을 재적용하여 반영되도록 설계한다. ESM(통합보안관리:Enterprise Security Management) 등 정보수집 모듈과의 연동 설계도 고려한다.

3.2.5 보안대상의 관리 방안
보안대상의 기본 관리 및 보안 대상 내 주요 오브젝트의 변경이력을 관리한다. 최근의 변경사항을 비교 이력으로 제공하며, 관리자 지정 특정 시점의 각 현황을 비교 분석하여 정보를 제공하며 정책관련 관리모듈을 제공한다.

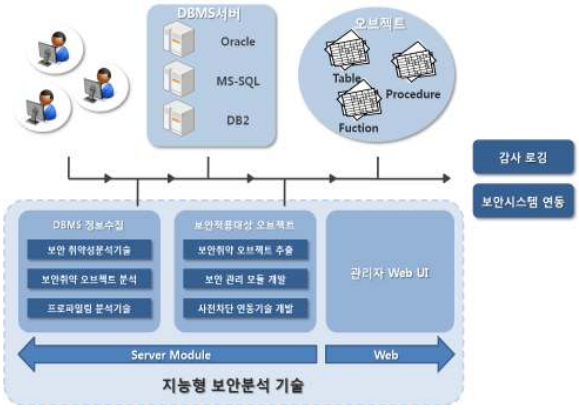

그림 2. 지능형 보안 분석 기술

3.3 모듈별 연관관계 및 프로세스
보안취약성 분석기술과 보안 취약 오브젝트 분석 기술을 통하여 보안적용 대상 오브젝트 생성하고, 보안적용 대상 오브젝트 및 프로파일링 분석결과를 관리하며 정책을 적용하도록 한다. 관리자 WEB UI(User Interface)를 통하여 관리 및 정책적용 등 시스템 제어를 수행한다. 이때 WEB UI에서 실시간 진행사항 등 데몬과의 통신이 필요한 부분도 같이 진행한다. 정책에 따라 운영된 결과 등을 감사 로깅하도록 하고, 연동이 필요한 부분은 연동모듈을 통하여 필요한 역할을 처리하도록 한다[5].

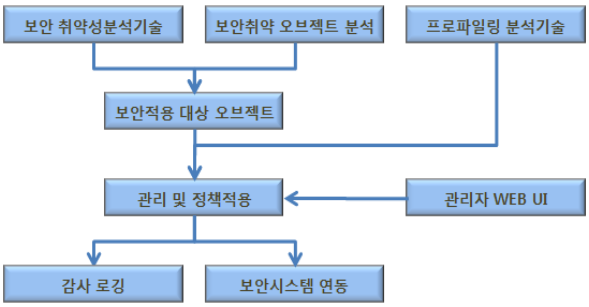

그림 3. 기능 연관도

Ⅳ. 결 론

본 논문의 연구 핵심은 그동안 해결하지 못한 보안취약 오브젝트에 대한 분석과 사용이력을 통한 권한의 오남용에 대한 탐지 및 제어 방안이다. 지능형 보안 분석 통하여 중요한 자산의 유출사

고나 해킹 등의 악의적인 목적에 의한 정보의 유출 및 파손을 사전에 예방하고 관리 한다.

이러한 기반 기술은 체계적인 정보유출 위험지수 관리, 보안취약 오브젝트의 관리, 보안 위협 사전 제거, 통합 관리의 편의성 등을 제공한다.

DB에 대한 전반적인 보안성을 높이는 지능형 보안 분석은 기존 시장에서 발생한 니즈를 반영한 것으로 기존 고객 및 신규고객을 통하여 새로운 영역의 보안시장이 창출될 뿐만 아니라 국내외 시장으로 넓혀 나 갈수 있을 것으로 예상된다.

향후 연구로는 DB 취약 오브젝트를 검출하여 분석하고, 분석된 정보를 이용해 실시간 보안관리 및 자동 점검하는 연구를 통해 정보보호기술의 검증수준을 극대화하겠다.

참고문헌

[1] Jong-Il Baek, "A Study on Traceback by WAS Bypass Access Query Information of Database," Journal of The Korea Society of Computer and Information, Vol.14, No.12, pp.181-190, Dec. 2009.

[2] Jong-Il Baek, "A Study on DB Security Problem Improvement of DB Masking by Security Grade," Journal of The Korea Society of Computer and Information, Vol.14, No.4, pp.101-108, Apr. 2009.

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

[4] Young-Lok Lee, "Design of Database Security Audit Format for Privacy Protection," Journal of The Korea Society for Internet Information, Vol.9, No.2, pp.119-124, Nov. 2008.

[5] Hyung-Jin Mun, "Sensitive Personal Information Protection Model for RBAC System," Journal of The Korea Society of Computer and Information, Vol.13, No.5, pp.103-110, Sep. 2008.

[6] KOREA FINANCIAL TELECOMMUNICATIONS & CLEARINGS INSTITUTE, "Analysis of the Status and Problems of DB security technology," Information Security Conference 2007, Sep. 2007.

[7] Jung-Ho Im, "Analyses on Standard Formats of Spatial Imagery Information," The Journal of GIS Association Of Korea, Vol.9, No.1, pp.31-50, Apr. 2001.