情報保護學會論文誌
第17卷 第1號, 2007. 2

접근제어형 데이터베이스 보안 시스템의 보호프로파일*

전 웅 렬,† 조 혜 숙, 김 승 주, 원 동 호‡
성균관대학교 정보통신공학부 정보보호연구소

A Protection Profile for Access Control Based Database Security System

Woongryul Jeon†, Heasuk Jo, Seungjoo Kim, Dongho Won‡
Information Security Group, Sungkyunkwan University

요 약

실생활에서 네트워크가 차지하는 비중이 점점 커지면서 데이터가 집약되어있는 데이터베이스 보안의 중요성도 점점 증가하고 있다. 현재 데이터베이스 보안은 크게 사용자 접근제어 방식과 데이터의 암호화 저장방식으로 구분된다. 그러나 데이터베이스 보안시스템에 대한 범용의 보호프로파일이 아직 존재하지 않기 때문에 정확한 평가가 어렵다. 이에 본 논문은 사용자 접근제어 형 데이터베이스 보안시스템의 보안기능요구사항을 개발한다. 본 논문은 접근제어 형 데이터베이스 보안시스템이 갖춰야 할 기본적인 필수기능을 제안한다. 이는 데이터베이스 보안시스템 평가 시 참고자료로 충분히 활용될 수 있을 것이다.

ABSTRACT

With increasing the amount of processed information over the network, the importance of database system increases rapidly. There are two types of security system for database, access control and data encryption. However, it is hard to evaluate security of database systems using the Common Criteria(CC) as there is no protection profile(PP) for these systems. In this paper, we propose a protection profile for secure database systems which can be used in formal evaluation using the Common Criteria. The proposed protection profile can be used by both developer and consumer to evaluate security of database systems.

Ⅰ. 서 론

데이터베이스 보안은 저장된 정보를 인가되지 않은 변경, 파괴, 노출 및 비일관성을 야기하는 사건으로부터 보호하는 것이다. 현대 사회에서 네트워크가 차지하는 비중이 높아지면서 대규모 개인 정보를 저장하는 데이터베이스의 보안 역시 중요한 요소로 부각되고 있다.[1]

데이터베이스 보안은 크게 두 가지 방식으로 구분할 수 있다. 하나는 사용자의 접근제어를 통해 데이터베이스의 보안을 도모하는 방식이고, 다른 하나는 데이터베이스 자체의 암호화를 통해 보안을 도모하는 방식이다. 하지만 데이터베이스 보안시스템에 대한 범용 보호프로파일의 부재로 인해 데이터베이스 보안시스템에 대한 명확한 평가가 어렵다. 이에 본 논문은 사용자 접근제어

접수일: 2007년 1월 16일; 채택일: 2007년 2월 7일
* 본 연구는 정보통신부 및 정보통신진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
† 주저자, wrjeon@security.re.kr
‡ 교신저자, dhwon@security.re.kr

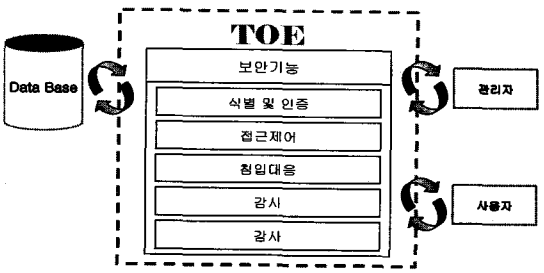
형 데이터베이스 보안시스템의 보안기능요구사항을 도출하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 보호프로파일과 데이터베이스 보안제품에 대해 알아보고, 3장에서는 TOE를 정의하고 TOE와 TOE의 환경에 적합한 보안기능요구사항을 도출한다. 4장에서는 도출한 보안기능요구사항이 TOE의 안전한 운영을 보장함을 증명하고, 5장에서 논문의 결론에 대해 기술한다.

Ⅱ. 관련연구

2.1 보호프로파일

보호프로파일은 공통평가기준에 기반한 정보보호제품의 평가에서 기초가 되는 문서로 소비자가 잠재적 제품에 대한 요구사항을 기술한 문서이다. 여기서 공통평가기준은 정보보호제품의 평가를 위한 국제표준을 말한다. 개발자는 보호프로파일을 토대로 소비자의 요구에 적합한 정보보호제품을 개발하고, 보안목표명세서를 통해 제품이 보호프로파일을 정확히 만족하는지 증명한다. 보안목표명세서는 TOE의 평가를 위한 근거로 사용하는 보안요구사항과 구현명세의 집합으로 특정 제품을 대상으로 한다. 보호프로파일은 크게 5장으로 나눌 수 있다. 1장은 평가의 대상이 되는 TOE의 정의와 TOE의 범위 및 TOE에 대한 설명을 담고 있다. 2장은 TOE를 운영할 환경에 대한 기술이다. 보안환경은 크게 가정사항, 위협, 조직의 보안정책으로 나누어 기술할 수 있다. 3장은 보안목적으로 TOE가 가져야 할 보안기능을 추상적으로 제시한다. 4장은 보안요구사항으로 보안기능요구사항과 보증요구사항으로 나누어진다. 4장은 3장에서 제시한 보안기능을 구체화하는 요구사항을 포함한다. 5장은 이론적 근거로 보안목적과 보안요구사항이 정확히 도출되었음을 증명하는 장이다.



〔그림 1〕 TOE

2.2 접근제어형 데이터베이스 보안시스템

접근제어 형 데이터베이스 보안시스템은 크게 두 가지 방법으로 사용자의 접근을 제어한다. 하나는 Gateway 방식이고 다른 하나는 Sniffing 방식이다. 본 논문은 Sniffing 방식의 사용자 접근제어 형 데이터베이스 보안시스템의 보호프로파일 개발을 목적으로 한다.

Sniffing 방식은 데이터베이스 보안 시스템이 데이터베이스에 접근하는 모든 사용자의 질의, 응답을 감시하는 방식이다. 사용자는 식별 및 인증과정을 거친 후 데이터베이스에 접근할 수 있으며 허가된 행위를 하는 한 보안시스템의 제지를 받지 않는다. Sniffing 방식은 데이터베이스의 가용성 확보에 유리하지만 공격에는 취약하다. 공격을 조기에 인지하고 즉각 대처하지 않는 한 공격 이후의 대처방안을 마련하는 것이 전부이기 때문이다.[2]

Ⅲ. 보안기능요구사항 도출

3.1 TOE

TOE는 Targer Of Evaluation의 약자로 평가의 대상인 IT 제품이나 시스템, 이와 관련된 설명서를 의미한다.[3] 본 논문에서 TOE는 접근제어 형 데이터베이스 보안시스템이다. 〔그림 1〕은 TOE와 그 기능을 나타낸다.

본 논문에서 TOE는 사용자의 접근을 제어하는 방식으로 데이터베이스를 보호한다. TOE는 데이터베이스에 접근하는 사용자를 식별 및 인증하고 사용자와 데이터가 주고받는 모든 데이터를 감사 및 관리한다.

3.2 TOE 보안기능

TOE의 주요 보안기능은 식별 및 인증, 접근제어, 침입대응, 감사, 감시기능이다. 아래 〔표 1〕은 보안기능에 대한 설명을 나타낸 것이다.

3.3 TOE 보안환경

TOE 보안환경은 TOE가 사용되는 환경을 정의한다. 정의는 가정사항, 위협, 조직의 보안정책, 이렇게 세 가지로 구분된다. 가정사항은 TOE의 보안목적이 성립하기 위한 필요조건이다.[4] 위협은 TOE 및 TOE의 운영

〔표 1〕 TOE의 보안기능

보안기능	개요
식별 및 인증	TOE는 사용자의 신원을 식별하고 인증한 후 접근여부를 결정한다.
접근제어	인가된 사용자만이 데이터베이스에 접근할 수 있으며, 허가된 명령만 사용할 수 있다.
침입대응	TOE는 악의적 사건에 대해 관리자가 사전에 설정한 대응책을 수행한다.
감시	TOE는 데이터베이스와 사용자간의 모든 데이터를 감시한다.
감사	TOE는 감사 가능한 모든 사건들을 감사기록하고, 허가된 사용자의 요청 시 감사기록의 정렬, 요약과 같은 기능을 제공한다.

환경에 위험을 초래할 수 있는 모든 요소를 의미한다. 그리고 조직의 보안정책은 TOE를 운영하는 조직이 갖추고 있는 내부의 보안정책을 의미한다.[5] 위협은 보안목적과 대응하며 가정사항 및 조직의 보안정책은 환경에 대한 보안목적과 대응한다. 〔표 2〕는 본 보호프로파일을 수용하는 TOE의 운영환경에 적용되는 가정사항, 위협, 조직의 보안정책을 나타낸다.

TOE 보안환경은 IT 보안요구사항의 기반이 되기 때문에 분석과정의 정교함이 요구된다. IT 보안요구사항은 TOE 보안환경에서 분석한 위협에 대응하고 가정사항 및 조직의 보안정책을 보강하기 위한 보안요구사항이기 때문이다.

3.4 보안목적

보안목적은 TOE 보안환경에서 식별된 모든 위협에 대응하기 위한 추상적인 목적으로 다음 장에서 이어질 보안기능요구사항에 의해 구체화된다. 보안목적은 TOE 보안목적과 환경에 대한 보안목적으로 나누어지는데, 환경에 대한 보안목적은 비 기술적/절차적 수단으로 충족할 수 있다.[6] 본 논문은 다음 장에서 TOE 보안목적에 대한 보안기능요구사항을 도출하며, 환경에 대한 보안목적은 다루지 않는다. 아래 〔표 3〕은 표 2를 토대로 도출한 보안목적을 나타낸 것이다.

〔표 2〕 보안환경

가정사항	위협	조직의 보안정책
A.물리적보안	T.반복인증시도	P.감사
A.신뢰된관리자	T.감사기록 실패	P.안전한관리
A.운영환경의 보안강도	T.가장	
	T.TOE 보안기능 우회접근	
	T.감사기록 손실	
	T.TOE 보안기능 데이터 손실	
	T.오용	

〔표 3〕 보안목적

TOE 보안목적	환경에 대한 보안목적
O1.가용성	OE.물리적 보안
O2.감사	OE.신뢰된 관리자
O3.관리	OE.운영환경의 보안강도
O4.식별 및 인증	
O5.TOE 보안기능 데이터 보호	

3.5 IT 보안요구사항

보안요구사항은 보안목적을 충족하기 위한 TOE 및 IT 환경의 요구사항이다. TOE 및 IT 환경은 보안요구사항의 이행을 통해 보안목적을 달성하며, 보안요구사항은 모든 보안목적을 충족해야 한다. 〔표 4〕는 〔표 3〕에서 도출한 보안목적을 만족하기 위한 보안기능요구사항을 나타낸다.

Ⅳ. 이론적 근거

본 장에서는 도출한 보안기능요구사항이 모든 보안목적을 달성하는지를 확인한다. 〔표 5〕는 〔표 4〕의 보안기능요구사항이 〔표 3〕의 보안목적을 어떻게 충족하는지를 증명한다.

〔표 4〕 보안기능요구사항

보안기능 클래스	보안기능 컴포넌트	
보안감사	FAU_ARP.1	보안경보
	FAU_GEN.1	감사 데이터 생성
	FAU_GEN.2	사용자 신원 연관
	FAU_SAA.1	잠재적인 위반 분석
	FAU_SAR.1	감사 검토
	FAU_SAR.3	선택가능한 감사 검토
	FAU_SEL.1	선택적인 감사
	FAU_STG.1	감사증적 보호
	FAU_STG.3	감사 데이터 손실 예측시 대응 행동
	FAU_STG.4	감사 데이터의 손실 방지
식별 및 인증	FIA_AFL.1	인증 실패 처리
	FIA_ATD.1	사용자 속성 정의
	FIA_UAU.1	모든 행동 이전에 사용자 인증
	FIA_UAU.4	재사용 방지 인증
	FIA_UAU.7	인증 피드백 보호
	FIA_UID.1	식별
보안관리	FMT_MOF.1	보안기능 관리
	FMT_MTD.1	TSF 데이터 관리
	FMT_MTD.2	TSF 데이터 한계치의 관리
	FMT_SMF.1	관리기능 명세
	FMT_SMR.1	보안역할
TSF 보호	FPT_AMT.1	추상기계 시험
	FPT_FLS.1	장애시 안전한 상태 유지
	FPT_RVM.1	TOE 보안정책 우회 불가성
	FPT_SEP.1	보안기능 영역 분리
	FPT_STM.1	신뢰할 수 있는 타임스탬프
	FPT_TST.1	TSF 데이터 보호
	FPT_TST.2 (확장)	TSF 데이터 무결성 오류 발생시 대응방법
자원 활용	FRU_FLT.1	오류에 대한 내성
	FRU_RSA.1	최대 할당치
안전한 경로/채널	FTP_ITC.1	TSF간 안전한 채널

〔표 5〕 이론적 근거

보안목적 / 보안기능 요구사항	O1	O2	O3	O4	O5
FAU_ARP.1		X			
FAU_GEN.1		X			
FAU_GEN.2		X			
FAU_SAA.1		X			
FAU_SAR.1		X			
FAU_SAR.3		X			
FAU_SEL.1		X			
FAU_STG.1		X			
FAU_STG.3		X			
FAU_STG.4		X			
FIA_AFL.1				X	
FIA_ATD.1		X		X	
FIA_UAU.1				X	
FIA_UAU.4				X	
FIA_UAU.7				X	
FIA_UID.1				X	
FMT_MOF.1	X		X		
FMT_MTD.1					X
FMT_MTD.2	X				
FMT_SMF.1			X		
FMT_SMR.1				X	
FPT_AMT.1	X				X
FPT_FLS.1	X				
FPT_RVM.1	X				X
FPT_SEP.1					X
FPT_STM.1		X		X	
FPT_TST.1	X				X
FPT_TST.2(확장)	X				X
FRU_FLT.1	X				
FRU_RSA.1	X		X		
FTP_ITC.1			X		X

V. 결 론

본 논문은 접근제어 형 데이터베이스 보안시스템의 보안기능요구사항을 도출하였다. 본 논문은 접근제어 형 데이터베이스 보안시스템의 보안요구사항을 도출하기 위해 TOE를 정의하고, TOE의 환경을 분석한 후, 환경에 적합한 보안목적을 도출하였다. 보안목적을 바탕으로 보안기능요구사항을 정의하였으며, 요구사항이 보안목적을 충족함을 이론적 근거를 통해 나타내었다.

본 논문은 접근제어 형 데이터베이스 보안시스템이 갖추어야 할 기본적인 필수보안기능을 제시하였다. 또한 본 논문은 데이터베이스 보안시스템의 평가 시 참고자료로 충분히 활용될 수 있을 것이다.

참고문헌

〔1〕 Min-A Jeong, Jung-Ja Kim, Yonggwan Won, "A Flexible Database Security System using Multiple Access Control Policies", PDCAT' 03 Proceeding, pp236-240, 2003.

〔2〕 E. Bertino and R. Sandhu, "DatabaseSecurity-Concepts, Approaches and Challenges", IEEE Transactionson Dependable and Secure Comp- uting, Vol2, No1, 2005.

〔3〕 Common Criteria for Information Technology Security Evaluation, Version 2.3, CCMB, 2005. 8.

〔4〕 이준호, 김영태, 이완석, "네트워크 스팸메일 차단시스템 보호프로파일 개발에 관한 연구, 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호", 한국정보처리학회, 1519-1532, 2006. 11.

〔5〕 홍원순, 김영태, 이완석, "기업용 바이러스차단 소프트웨어 보호프로파일에 대한 연구", 한국정보처리학회 추계학술발표대회 논문집 제13권 제2호", 한국정보처리학회, 1541-1544, 2006. 11.

〔6〕 국가기관용 침입탐지시스템 보호프로파일 V1.2, 국가정보원, 2006. 5

〔7〕 Common Methodology for Information Technology Security Evaluation Part 2, Version 2.3, CCMB, 2005. 8.