데이터베이스 보안 위협 및 고찰

주재웅 [1], 박종혁 [1*]
서울과학기술대학교 컴퓨터공학과
[1]e-mail : {woong07, jhpark1}@seoultech.ac.kr

Security threats and Review for Database

Jae Woong Joo[1], Jong Hyuk Park[1*]
Dept. of Computer Science and Engineering and Dept. of Interdisciplinary Bio IT Materials,
SeoulTech, Korea

요 약

데이터베이스 보안은 외부자나 내부자가 데이터베이스 및 데이터베이스 내에 저장된 데이터를 비인가 된 변경, 파괴, 노출 및 비 일관성을 발생시키는 사건이나 위협들로부터 보호하는 것이다. 이러한 DB 의 보안위협들은 사용자의 실수, 오용, 내부자의 권한 남용, 비정상적인 접근행위 등 DB 에 대해 알려진 보안 취약점들로부터 발생한다. 본 연구에서는 데이터베이스 보안의 고려사항과 연구동향에 대해 살펴보고 현재 데이터베이스 분야에서 보안이 적용된 시스템에 대해 분석하고 취급되는 정보보호의 중요성에 대해 고찰한다.

1. 서론

데이터베이스 보안은 허가 받은 사람이 허가된 권한으로 허가된 자료 및 자원에 대해서 사용하고, 비인가 된 사용자가 자료 및 자원에 대해 접근, 사용, 노출, 파괴, 변경, 탐색 및 비 일과성을 발생시키는 것을 방지하는데 목적이 있다 [1].

그러나, 인터넷으로 인한 네트워크 개방으로 IT 와 정보화의 급속한 성장으로 피해 규모 확대 및 피해 확산 속도가 빨라졌다. 또한 지적 재산이 기업의 생존과 직결되어 있으며 보안 사고 발생 시 피해 복구, 소송 등 막대한 비용 발생으로 기업과 개인 모두에게 심각한 피해를 입히는 행위 또한 해마다 급증하고 있다. 더구나 스마트기기가 대중적으로 확산되고 모바일 오피스가 빠르게 도입됨에 따라 PC 환경에서 나타났던 보안 위협이 스마트기기 환경으로 이동하여 정보유출 위협까지 함께 증가하고 있다. 또한 어플리케이션 및 데이터베이스 설계 시 다양한 보안문제를 감안하지 않고 구축의 편의성을 위해 데이터베이스 보안 문제를 경시한 것이 문제가 되고 있다. 이러한 보안 문제를 해결하기 위한 서비스가 제공되어야 한다 [2].

본 논문에서는 데이터베이스 보안의 고려사항과 연구동향에 대해 살펴보고 현재 데이터베이스의 위협요소 및 악성코드 유형을 분석하여 정보보호의 중요성에 대해 고찰한다.

2. 보안 고려사항

데이터베이스 보안의 목적은 데이터베이스에 저장된 데이터를 공개, 노출, 변조, 파괴, 훼손, 지체, 재난 등의 위협으로부터 보호하여야 한다 따라서 기밀성, 무결성, 가용성에 대해 고려해야 한다. 본 장에서는 데이터베이스의 보안 고려사항에 대해 설명한다.

2.1 기밀성

선별적인 접근 체계를 만들어 비인가 된 개인이나 시스템에 의한 접근과 이에 따른 정보 공개/노출을 막는다. 접근 가능한 데이터를 선별하며, 데이터에 접근할 수 있는 자격을 분류하여 기밀성을 보장해야 한다.

2.2 무결성

접근제어와 의미적 무결성 제약을 함께 적용하여 보장해야 한다. 즉, 어떤 주체가 데이터를 변경하려고 할 때마다 접근 제어 메커니즘은 사용자가 데이터를 변경할 권한이 있는지를 검증하고, 의미적 무결성 서브시스템은 갱신된 데이터가 의미적으로 정확한지를 검증해야 한다.

2.3 가용성

DBMS 버그, 관리자 실수, 관리 절차 미준수, 악의적 공격 등으로 인한 지체, 접속불능 같은 서비스 장애를 예방하면서 항상 가용한 상태를 유지하여, 정당한 권한을 가진 사용자나 어플리케이션에 대해 원하는 데이터에 대한 접근을 제공하는 서비스를 지속할 수 있도록 보장해야 한다.

3. 데이터 베이스 위협과 보안위협

데이터베이스는 데이터베이스 위협과 보안위협이 있다.

3.1 데이터베이스 위협

데이터베이스의 위협은 3 가지가 있으며, 데이터의 부당한 검색, 수정, 삭제로 이뤄져 있다.

- **데이터 노출**
  기밀성의 반대로써, 부당한 사용자가 의도적이거나 우연히 접근하여 데이터의 일부 또는 전체가 유출함으로써 소유자나 관리자의 의사에 반하여 정보가 유출되는 것이다 [3].
- **데이터의 부적절한 변경**
  데이터가 정당한 권한을 가진 사용자나 애플리케이션 또는 프로세스에 의해 변경되지 않고 부당한 방법이나 절차에 의해 변경된 것을 의미한다. 이것은 데이터 무결성에 관련된 모든 위반이다 [3][4].
- **서비스 거부**
  데이터베이스에 대한 서비스 거부는 데이터베이스의 세션자원을 소진시켜 접속을 못하게 하거나, 오동작을 유발시키고 작동 불능 상태를 유발함으로써 데이터베이스를 셧다운시키거나 무한정의 대기 상태를 유발하여 데이터베이스 서비스를 방해하는 행위들이 해당된다 [3].

데이터베이스 위협에 대한 보안 요구사항은 <표 1>과 같다[3,4].

<표 1> 데이터베이스 위협 및 요구사항

데이터베이스 위협요소	데이터베이스 보안 요구사항
데이터 노출	기밀성
데이터의 부적절한 변경	기밀성, 무결성, 가용성
서비스 거부	가용성

3.2 데이터베이스 보안위협

데이터베이스 보안 위협은 우연적 위협과 의도적 위협으로 나눌 수 있다. 우연적 위협은 손상을 주려는 의지가 아닌 뜻밖의 사고로서 다음과 같은 유형이 있다.

- 지진이나 수해 혹은 화제와 같은 천재지변이나 우발 재해의 사고는 시스템 하드웨어나 저장 데이터를 손상시킬 수 있으며, 무결성 위반이나 서비스 거부를 일으킬 수 있다 [3].
- 하드웨어나 소프트웨어에서의 오류나 버그로 인하여 데이터의 비권한 접근, 수정 등이 발생할 수 있으며, 권한 있는 사용자가 접근거부를 당할 수도 있다 [5, 6].

의도적 위협은 정보의 유출 및 손상을 주려는 확실한 의지에 의해 발생하는 것을 말한다.

- 인가된 데이터베이스 사용자, 데이터베이스 관리자, 네트워크/시스템관리자를 비롯한 비인가 된 사용자나 해커 등에 의해 우발적 또는 고의적으로 발생하는 비인가된 활동이나 오용 [6, 7].
- 고의적으로 인가된 사용자가 데이터베이스를 사용할 수 없도록 만드는 과부하, 성능제약, 용량문제 등과 같은 사고를 유발하는 악성코드 감염 [6].

4. 결론 및 고찰

본 논문에서는 데이터베이스 보안 고려사항과 데이터베이스 위협과 보안위협에 대해 논의하였다.

IT 의 발전으로 인해 데이터가 클라우드화되고 빅데이터화되면서 거대해지고 복잡해지고 있다. 이러한 데이터들을 분석하여 사용자가 어떤 정보를 필요로 하는지 맞춤형 서비스가 제공되어야 한다. 또한 데이터의 양이 너무 거대해지면 특정 데이터가 어떤 사용자의 것인지 섞여서 불특정한 사용자들에게 제공하는 문제가 발생할 수도 있다. 전세계 수많은 사용자들을 대상으로 서비스를 제공하므로 굉장히 많은 경우의 수와 불특정한 사람들 사이에서 어떻게 보안을 해야 할 것인지 고려해야 한다 [8]. DB 사용자의 행동을 감시하여 누가 어떤 테이블을 언제 사용하고, 어떤 작업을 하는지를 기록하는 효율적인 보안 감사기능과 DB 내의 중요 데이터의 손실을 방지하는 효과적인 보안 기법을 연구해야 할 것이다.

Acknowledgment

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1014)

참고문헌

[1] Kadhem H, Amagasa T, Kitagawa H, “A Novel Framework for Database Security based on Mixed Cryptography”, Internet and Web Applications and Services, 2009, ICIW 09. Fourth International Conference on, Publication Year, 2009, pp. 163 – 170.

[2] Luc Bouganim, Yanli GUO, “Database Encryption”, Encyclopedia of Cryptography and Security, 2009, pp. 1-9.

[3] 노시춘, "Data Base 보안과 Oracle 보안 구현."융합보안논문지 Vol. 3, No.3, 2003, pp.7-18.

[4] Yan, Yi, Su Zhengyuan, Dai Zucheng, "The database protection system against SQL attacks."Computer Research and Development (ICCRD), 2011 3rd International Conference on. Vol. 3, IEEE, 2011.

[5] Mohamed, Mohamed A., Obay G. Altrafi, and Mohammed O. Ismail, "Relational vs. NoSQL Databases: A Survey.", International Journal of Computer and Information Technology, ISSN.2279–0764, Vol. 2014.

[6] Van der Veen, Jan Sipke, Bram Van der Waaij, Robert J. Meijer, "Sensor data storage performance: Sql or nosql, physical or virtual.", Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on. IEEE, 2012.

[7] 장승주, 김성진. "Oracle 특정 IP 보안취약점에 관

한 연구."한국통신학회 종합 학술 발표회 논문집 (동계) 2014, pp.392-394.
[8] 이병엽, 임종태, 유재수, “데이터베이스 암호화 솔루션 구현 및 도입을 위한 기술적 아키텍처”, 한국콘텐츠학회논문지, Vol. 14, No. 6, 2014, pp.1-10.