일반화된 연관 패턴을 이용한 사용자 비정상행위 탐지에 관한 연구

이현화* 오상현 이원석
{swanlee*, osh, leewo}@amadeus.yonsei.ac.kr
연세대학교 컴퓨터과학과 데이터베이스 연구실
Tel. 02-2123-2716

키워드 : 데이터베이스 보안, 데이터마이닝,
일반화된 연관 패턴, 비정상행위 탐지

요 약

최근 정보통신의 발전과 더불어 시스템 침투 기법도 고도화되고 전문적으로 변해가고 있다. 네트웍을 통한 시스템의 파괴 및 서비스 거부 유발 행위 등 컴퓨터를 이용한 침입 및 범죄로 인한 피해와 같은 통신 기술 발전의 부작용이 나타나고 있다. 이러한 시스템 침입 유형은 다양화되고 있으며, 기밀정보 유출과 같은 내부 권한 오용자에 의한 손실도 크게 증가하고 있다. 이에 운용체제와 네트워크 보안에 관한 연구는 활발히 진행되고 있으나, 중요데이터가 저장되고 있는 데이터베이스에 대한 보안은 데이터베이스 관리시스템에만 의존하고 있는 실정이다. 이러한 이유로 데이터베이스 사용자의 계정 도용 및 권한 오용 등의 정보유출은 탐지가 힘들다.

따라서, 본 논문에서는 방대한 로그 데이터의 지능적이고 자동적인 분석을 위해 사용자 로그 데이터의 계층구조를 고려하여 연관 패턴을 생성해 낸다. 효율적인 정상행위 패턴 생성을 위해 프로그램 사용자, 대화환경 사용자를 구별하여 모델링 하며, 이를 이용하여 외부 침입자 및 내부 권한 오용자에 대한 침입 탐지를 수행한다.

본 연구는 비정상행위 판정을 위해 크게 오프라인 작업과 온라인 작업으로 나뉘며, 오프라인 작업에서는 사용자의 로그 데이터를 추출하여 데이터베이스 사용자들의 행동 패턴에 관한 자료를 추출하고, 데이터 마이닝 기법을 이용하여 사용자별 고유한 정상행위 패턴을 찾는다. 이때 데이터 마이닝 기법 중에 하나인 연관 규칙을 적용한다. SQL문이 갖는 특성을 반영한 계층구조를 갖는 데이터에 적용 가능한 일반화된 연관 패턴 생성 알고리즘을 사용한다. 또한 사용자별 작업 환경을 구분함으로써 효율적인 프로파일을 생성한다. 일정기간 동안의 사용자 로그 데이터를 SQL문장 추출기를 통하여 자동으로 추출해 내며, 추출된 SQL문장은 파서를 통해 생략된 문장이 보충되며, 패턴 트리 생성기를 통해 계층구조를 갖는 패턴 트리를 형성하고, 최종적으로 프로파일 추출기를 통해 정상행위 프로파일을 생성한다.

온라인 작업에서는 오프라인 작업에서 만들어진 사용자별 프로파일 데이터베이스를 이용하여 사용자가 SQL문 수행 시 파서를 통해 코드화 변환과정을 수행하게 되며 이때 생성된 코드가 해당 사용자의 정상행위 프로파일에 존재한다면, 존재하는 SQL문과 같은 문장으로 인식됨으로써 정상행위에 포함되는 반면 존재하지 않을 경우 비정상행위로 판정하는 사용자의 비정상행위를 탐지하는 비정상행위 판정 모델을 개발한다. 사용자가 수행한 SQL문장에 대해 정상행위도, 비정상행위도를 정의하며, 이 값의 변화를 인지함으로써, 타인의 계정을 도용하거나 자신이 조작할 수 없

는 분야에 접근할 경우 비정상행위로 판정할 수 있다. 결과적으로 외부 침입자와 함께 내부 권한 오용자의 비정상행위를 탐지 할 수 있다.