난수 패스워드를 이용한 데이터베이스 보안 시스템의 설계 및 구현

이화민[O] 이원규 유헌창 김현철
고 려 대 학 교 컴 퓨 터 교 육 과
{zelkova, lee, yuhc, hkim}@comedu.korea.ac.kr

Design and Implementation of Database Security Using Random Number Password

Hwa-Min Lee[O] Won-Gyu Lee Heon-Chang Yu Hyeon-Cheol Kim
Dept. of Computer Science Education, Korea University

요 약

최근 컴퓨터 기술 발달과 데이터 통신의 발전으로 여러 사용자가 데이터와 정보를 공유하게 되고 데이터의 전송, 수집, 검색, 수정 등의 업무가 많아짐에 따라 데이터베이스에 대한 보안의 중요성이 더욱 증대되고 있다. 따라서, 본 논문에서는 패스워드를 이용한 인터페이스 보안과 보안 요소들을 계층별로 나누고 사용자 등급을 이용한 내적 보안을 혼용하여 기존의 패스워드 데이터베이스 보안 시스템의 문제점을 보안하는 난수를 이용한 데이터베이스 보안 시스템을 설계하고 구현하였다.

1. 서론

현대 사회가 정보화 사회로 변환되어 가면서 많은 양의 정보와 데이터를 효율적으로 관리하기 위해서 데이터베이스 관리 시스템(DBMS : database management system)의 이용이 증가하고 있다. 데이터베이스 관리 시스템이 파일 시스템에 비해 지니는 장점으로는 데이터의 공용과 데이터의 중복의 최소화로 데이터의 무결성을 보장할 수 있다는 것이다[1,2]. 데이터베이스 관리 시스템은 여러 사용자에게 필요한 데이터를 저장장치에 저장하고 이 정보들을 전체적으로 관리하는데, 데이터의 공유 때문에 보안에 관한 문제점이 발생하게 된다.

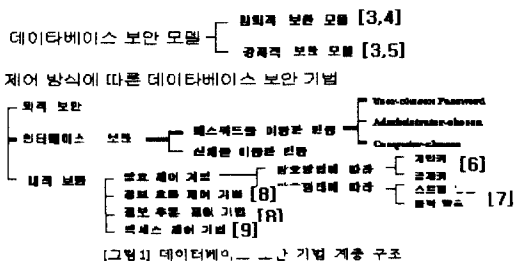
이 논문에서는 데이터베이스 보안 방법 중에서 기존의 패스워드 시스템에서 사용하는 기본 패스워드에 부가적으로 시스템의 시간을 이용한 난수 패스워드를 추가하여 두 개의 패스워드를 추가하여 두 개의 패스워드를 사용함을 통해 데이터베이스의 보안을 증대시키는 데이터베이스 보안 시스템을 설계하였다.

이 논문은 제2장에서 여러 가지 데이터베이스 보안 기법에 대해 정리와 함께 패스워드를 이용한 데이터베이스 보안에 대해 소개하고, 제3장에서는 제안한 난수 패스워드 시스템의 구조 및 기능 그리고 제어 과정을 설계 제안하였다. 제4장에서는 난수 패스워드를 이용한 데이터베이스 보안 시스템의 성능을 분석하고 제5장에서 앞으로 연구할 과제를 제시하였다.

2. 관련 연구

2.1 데이터베이스에서의 보안 기법

데이터베이스 보안 기법의 전반적인 계층 구조는 [그림1]과 같다.



[그림1] 데이터베이스 보안 기법 계층 구조

2.2 패스워드를 이용한 보안 대책

2.2.1 패스워드의 성격과 종류

패스워드는 데이터의 시큐리티와 동기, 제한, 감시 감독 등과 같은 여러 형태의 관리요구 전반에 있어서 기초가 된다. 패스워드는 데이터베이스와 사용자간에 열쇠의 역할을 위해 만든 것으로 사용자와 시큐리티 데이터베이스 시스템간에 외적인 접근 제어를 가능하게 한다. 패스워드 종류에는 사용자가 스스로 패스워드를 선택하는User-chosen password, 데이터베이스 시큐리티 관리자에 의해 모든 패스워드가 만

들어지고 운영되는 방식인 Administrator-chosen password, 컴퓨터가 패스워드를 만들어 내는 방식 Computer-chosen password가 있다.

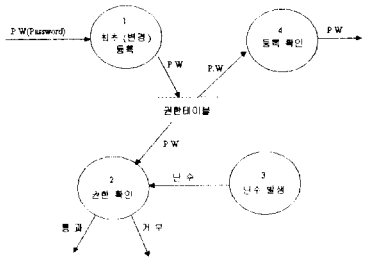
2.3.3 패스워드 노출과 보안 대책

침입자가 사용자의 패스워드를 부당하게 획득하여 데이터베이스 시스템을 사용하는 경우에는 다음과 같은 것들이 있다. 시스템의 패스워드 파일을 판독하는 경우인 시스템 내부에 저장되어 있는 패스워드 정보에 접근하여 획득, 사용자가 데이터베이스 시스템과 통신 중에 가로채는 방법, 쉽게 추측될 수 있는 패스워드를 선택한 경우와 같은 사용자의 부주의로 인한 패스워드 노출이 바로 그것이다.

이러한 패스워드 노출에 따른 보안 대책으로는, 첫 번째의 경우, 패스워드를 다음과 같이 암호화함으로서 해결될 수 있다. Y=F(X), 즉 주어진 패스워드 X는 F(X)라는 알고리즘에 의해 변형된 후, Y라는 값으로 시스템에 저장된다. 권한 확인시에는 사용자가 입력시킨 패스워드 X를 F(X)로 계산한 후 그 결과를 저장되어 있는 값 Y와 같은지를 비교한다. 두 번째의 경우, 패스워드의 사용순서를 X_1, X_2, ... , X_n 등으로 정함으로서 해결될 수 있다. $Y_i = F(X_i)$, 즉 모든 X_i에 대응하는 Y_i의 값을 시스템에 저장한다. 본인 확인시에는 사용자가 입력시킨 패스워드 X_i를 $F(X_i)$로 계산한 후, 그 결과를 저장되어 있는 값 Y_i와 같은지를 비교한다. 사용자가 X_i session을 사용 후에는 다음에 사용될 패스워드 Y_{i+1}를 시스템에 통보된다. 세 번째의 경우는, 어떤 패스워드 시스템에서도 해결될 수 없다. 왜냐하면 시스템에서는 구별할 수 없는 동일한 패스워드가 각기 다른 사용자에 의해 사용될 수 있기 때문이다. 따라서 이를 방지하기 위해서는 음성인식이나 지문인식 등과 같은 물리적인 권한 확인 기법이 요구된다.

3. 난수 패스워드 시스템의 설계 및 구현

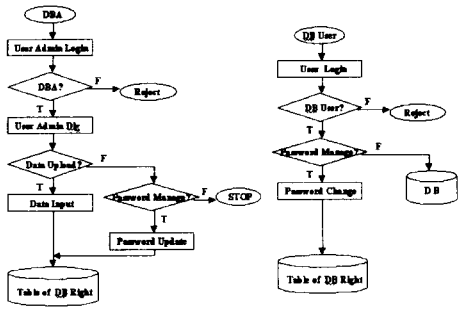
이 논문에서 제안한 난수 패스워드를 이용한 데이터베이스 보안 시스템의 구현은 windows98 환경에서 비주얼 C++를 이용하였으며, [그림2]와 같이 4개의 서브시스템으로 구성된다. 여기서 사용자나 데이터베이스 관리자가 보안 시스템을 통해 데이터베이스에 접근하고자 할 때, 시스템의 흐름은 [그림3]과 같이 두 가지 측면에서 고려할 수 있다.



[그림 2] 패스워드 시스템 구성

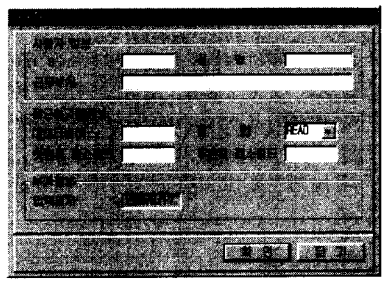
이제 보안시스템을 구성하는 4개의 서브 시스템의 기능을 설명하면 다음과 같다.

(1)최초(변경) 등록 서브 시스템 : DBA(database administrator)가 데이터베이스에 접근하는 사용자들에 대한 정보를 등록하는 시스템으로 서브 시스템의 구성은 [그림4]과 같다. 구분란에는 신규, 변경, 삭제 등 처리 구분을 입력하고, 권한란에는 DB 사용권한을 입력한다. 패스



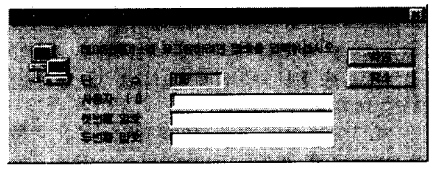
[그림 3] 데이터베이스 보안 시스템 흐름

워드1에는 기본 패스워드를, 패스워드2에는 난수 패스워드의 베이스 숫자를 입력하도록 구성되어 있고 입력된 내용은 권한 테이블에 등록이 되고 최초 등록일이 셋(set)되어 진다.



[그림 4] 등록 서브 시스템

(2)권한 확인 서브 시스템 : 사용자들이 데이터베이스에 접근하고자 할 때, 사용자의 ID와 암호를 이용하여 접속하는 로긴 서브 시스템으로 [그림5]와 같이 구성된다. 사용자가 특정 DB에 접근하고자 할 때는 이 화면을 통하여 패스워드 확인을 통과해야 하는데, 패스워드1에는 기본 패스워드를, 패스워드2에는 화면에 출력된 난수와 등록시킨 난수 패스워드의 베이스 숫자를 합한 숫자를 입력하여야 한다.



[그림 5] 사용자 권한 확인 서브 시스템

(3)난수 발생 서브 시스템 : 메인 프로그램(main program)의 호출에 의해 난수를 발생시키는데 난수 발생 절차는 다음과 같다.

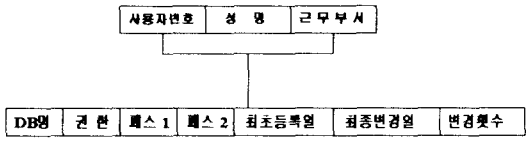
①시스템으로부터 HH.MM.SS(시, 분, 초)를 인수로 받아 HHMMSS를 제곱하여 11자리 숫자로 만든다.

②각 숫자에 소수로 구성된 weight를 곱한 후, 그 결과의 각 자리를 합하여 3자리 난수를 만든다.

③조합된 난수를 호출 프로그램으로 보낸다.

(4)등록 확인 서브 시스템 : 데이터베이스의 사용자의 정보를 등록확인하고 관리하는 서브 시스템이다.

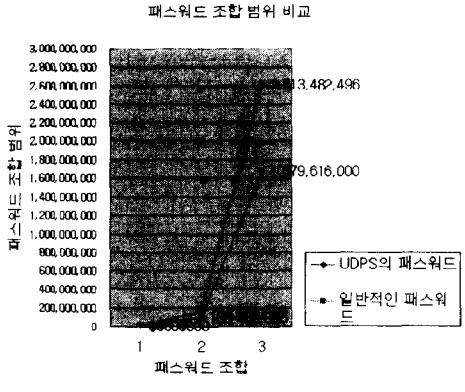
(5) 권한 테이블(table of right)의 구성은 [그림 7]과 같다. 사용자 번호와 DB명은 key 항목이 된다. 권한은 숫자(1 : READ, 2 : WRITE, 3: UPDATE, 4 : DELETE)를 이용한다.



[그림 6] 권한 테이블 구성

4. 성능 분석

난수 패스워드 시스템의 장점으로 첫째, 패스워드의 보안 증대는 난수 패스워드 시스템에서는 기본 패스워드 이외에 난수 패스워드를 부가적으로 사용을 할 수 있으므로 패스워드의 보안이 증대된다. 실제 제안된 시스템에서의 패스워드의 조합 범위는 기본 패스워드를 통한 조합 $n\Pi k$, 숫자3자리를 이용한 난수 패스워드의 조합범위가 최대출력 난수 557개 + 최대등록베이스숫자 ${}_{10}\Pi_3-1$으로 전체 패스워드의 조합 범위는 $n\Pi k * (557 + {}_{10}\Pi_3-1)$가 된다. 이에 반해 동일한 조건의 이란 패스워드 시스템에서의 조합범위는 기본 패스워드에 의한 조합 $n\Pi k$, 숫자 3자리를 이용한 조합이 ${}_{10}\Pi_3$으로 전체 패스워드의 조합 범위는 $n\Pi k * {}_{10}\Pi_3$이 된다. 따라서 제안된 시스템에서는 사용자가 기억하는 동일한 패스워드 길이로서 일반 패스워드 시스템보다 약 1.6배의 패스워드 조합범위를 얻을 수 있으며, 또한 난수 발생 서브 시스템에서 가중치를 높이면 최대 출력 난수가 커지므로 조합범위가 더욱 증대될 수 있다.



[그림 7] 패스워드 조합 범위

둘째, 통신회선 상에서 패스워드의 노출위험 감소는 일반 패스워드 시스템에서는 패스워드가 통신회선 상에서 도청될 수 있으므로 패스워드의 노출위험이 존재하지만 제안된 시스템에서는 패스워드가 통신회선 상에서 도청된다 하더라도 난수 패스워드가 부가적으로 존재하여 사용시마다 변경되므로 패스워드의 노출위험이 감소한다.

셋째, 장기간 패스워드의 변경이 없는 사용자에 대한 통제는 제안된 시스템에서는 DBA가 권한 테이블(table of right)에 기록된 최초등록일, 최종변경일, 변경횟수 등 패스워드 변경사항을 통하여 장기간 패스워드의 변경이 없는 사용자에 대하여 패스워드의 강제로 변경시키거나, 또는 데이터베이스의 사용권한을 회수하는 등의 필요한 조치를 취할 수 있다.

5. 결 론

이 논문에서는 데이터베이스의 보안을 증대시키기 위하여 부가적 난수 패스워드를 이용한 데이터베이스 보안 시스템을 제안하고 구현하였다. 기존의 데이터베이스 시스템에서는 사용자가 선택한 패스워드만을 이용하였지만 제안된 난수 패스워드를 이용한 데이터베이스 보안 관리 시스템은 데이터베이스에 접근을 통제하는 방식에 있어서 기존의 패스워드뿐만 아니라 시스템의 시간을 이용하여 발생시킨 난수를 이용한 패스워드를 부가하여 두 개의 패스워드를 사용하도록 하여 데이터베이스의 보안을 증대시켰다. 여기서 기존의 패스워드 시스템보다 하나의 패스워드를 추가로 사용해야 하는 부담감의 문제가 제기될 수 있는데 기본 패스워드가 4자리 숫자에 불과하고 난수 패스워드의 베이스 패스워드 역시 2자리 숫자이기에 기존의 4자리 이상 8자리 이하의 패스워드 시스템에 비하여 부담감은 증가하지 않는다. 또한 제안된 보안 시스템은 DBA를 위한 사용자 정보 등록 기능, 변경 기능, 삭제 기능과 함께 사용자를 위한 패스워드 변경 기능과 패스워드를 통한 데이터베이스 접근 통제 기능을 가지고 있다. 그리고 권한 테이블을 사용하여 각 데이터베이스마다 사용자의 접근 권한을 설정하여 권한을 가진 자만이 해당 데이터베이스에 접근할 수 있도록 하였다.
제안된 시스템은 데이터베이스와는 별도로 하나의 독립된 시스템으로 구현이 되어 있기 때문에 추후 네트워 기능을 추가하여 실제 데이터베이스와 연동하여 사용할 수 있도록 계속 연구하고자 한다.

5. 참고 문헌

[1]. John R. Campbell, "A Brief Tutorial on Trusted Database Management Systems," 13th NCSC Proc. Vol. II, 1990.
[2]. C. J. Date, An Introduction to Database System, Addison-Wesley, 1987.
[3]. R. Elmasri and T. F. Lunt. A Multilevel Relational Data Model. Proceedings of IEEE Symposium on Research in Security and Privacy, 1987.
[4]. R. Fagin, "On an Authorization Mechanism," ACM Transaction on Database Systems, 1978.
[5]. D. E. Denning and T. F. Lunt. A Multilevel Relational Data Model, Proceedings of IEEE Symposium on Research in Security and Privacy, 1987.
[6]. Dorothy E. Denning, Cryptography and Data Security, Addison-Wesley, 1982.
[7]. Goerge I. Davida and David L. Wells and Jhon B. Kam, "A Database Encryption System with Subkeys," ACM Trans. on Database System, Vol6, No.2, Jun. 1981.
[8]. C. P. Pfleeger, Security in Computing, Prentice-Hall, Inc. 1989.
[9]. Philip J. Pratt and Joseph J. Adamski, Database System : Management and Design, Boyd & Fraser Publishing Company, 1987.