분산 네트워크 환경하에서 암호화 된 사용자 인증 모듈을 적용한 데이터베이스 보안 시스템

이대영* 김옥환**

Study On Distribute Computing Network Security Using Encrypted User Security Module

Dae-Young Lee* Ok-Hwan Kim**

요 약

분산 컴퓨터 네트워크는 단일 시스템의 동작 정지로 인한 전체 시스템에 미치는 영향을 적게 함으로써 신뢰도를 높일 수 있고, 한 개의 대형 시스템을 활용하는 것 보다 저렴한 비용으로 보다 나은 성능을 얻을 수 있는 장점이 있다. 또한 시스템이 확장 및 재구성이 용이하다[1]. 그러나, 분산 컴퓨팅 환경에서 네트워크를 통한 데이터의 공유는 실생활이 되고 있는 반면 네트워크 환경에서 데이터의 무결성과 보안에 대한 위험성은 증가하고 있다[2][3]. 따라서 본 논문에서는 운영적 요소와 기술적 요소에 대한 분석을 통해 이러한 요소들을 결합시키기 위한 네트워크 암호화 데이터베이스 보안 시스템 모델을 제시한다. 제시한 모델에 운영적 요소와 기술적 요소를 체계적으로 결합시킨다면 분산 컴퓨팅 환경에서 허가받지 않은 사용자로부터 데이터를 안전하게 보호할 암호화 데이터베이스 보안 시스템을 구축할 수 있을 것이다.

ABSTRACT

This paper describes access control, user authentication, and User Security and Encryption technology for the construction of database security system from network users. We propose model of network encrypted database security system for combining these elements through the analysis of operational and technological elements. Systematic combination of operational and technological elements with proposed model can construct encrypted database security system secured from unauthorized users in distributed computing environment

키워드

Database security, Protection in Network Environment

Ⅰ. 암호화 된 사용자 보안 메커니즘

분산 컴퓨터 네트워크 환경에서 사용자 인증은 아이디와 비밀번호를 그대로 데이터베이스에 저장하므로 외부에 노출될 위험이 있어 보안이 취약하다. 이에 제안한 암호화 사용자 보안 시스템에서는 RSA 공개키 암호방식을 적용하여 아이디와 비밀번호를 암호화하여 데이터베이스에 저장하였다[그림 1][3]. 사용자 인증 시 암호화된 아이디와 비밀번호를 비교하여 확인하므로 보다 강력한 보안을 유지할 수 있고, 허가받은 사용자만이 효과적으로 정보자원을 이용할 수 있도록 설계하였다.

* 조선대학교 전산통계학과
** 목포해양대학교 해양전자통신공학과

접수일자 : 2005. 11. 11

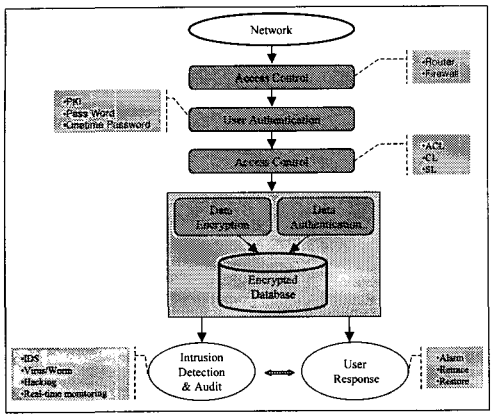


그림 1. 암호화 된 사용자 보안 메커니즘
Fig. 1. Encrypted database security system Model

1.1. 암호화 된 사용자 보안 소프트웨어 구성

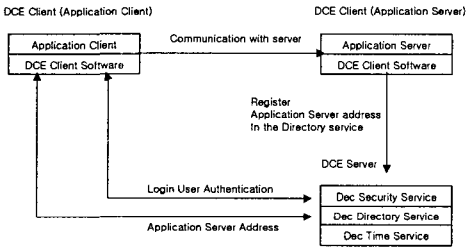


그림 2. 분산 컴퓨터 네트워크 환경에서 클라이언트와 서버와의 관계
Fig. 2. Relationship with server and client of distributed computing network

분산 컴퓨터 네트워크 환경에서 암호화 사용자 보안 시스템을 구현하기 위해 DCE 인증서버, DCE 클라이언트 애플리케이션 서버, DCE 클라이언트 애플리케이션을 구성할 수 있으며, 이들 상호간의 소프트웨어 관련 구성도는 [그림2]와 같다.

1.2. 암호화 된 사용자 인증 및 권한

분산 컴퓨터 네트워크 환경에서 암호화 사용자 인증은 일반적으로 DCE에서 제공하는 Kerberos에 의하여 이루어지며, 권한 확인은 DCE에서 제공하는 ACL 기능을 사용하여 구현한다. DCE Registry 데이터베이스는 각종 사용자 정보, 비밀번호 정보, ACL 정보를 저장한다. 클라이언트의 사용자 인증은 DCE의 Kerberos에 의하여 수행되고, 트랜잭션 업무 처리는 클라이언트가 수행하고 그 중간에 ACL을 통한 접근 통제는 DCE에 의해서 수행된다 [그림 3].

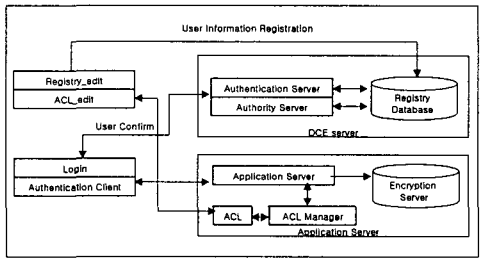


그림 3. DCE를 통한 암호화 사용자 인증 및 권한
Fig. 3. User authentication and authority of DCE

DCE를 통한 사용자 인증 및 권한 확인 절차는 다음과 같다.

step 1. 정보보호관리자는 Registry_edit를 이용하여 Registry 데이터베이스에 사용정보를 등록한다.

step 2. 어플리케이션 관리자는 ACL_edit를 이용하여 어플리케이션, 파일, 디렉토리등과 같은 객체에 대한 접근통제를 위하여 사용자, 그룹 등 이름을 만든다.

step 3. 사용자가 인증 서버에 login 할 때, login 프로세스는 다른 서버에 접근하기 위한 ticket을 얻기 위하여 사용자 확인을 거쳐 인증 및 권한 서버와 연결한다.

step 4. 인증서버와 권한은 Registy 데이터베이스로부터 사용자의 비밀키와 권한 속성을 얻어 사용자에 대한 인증을 하고, 다른 서버에 접근할 수 있는 증명서를 만든다.

step 5. 사용자가 어플리케이션 클라이언트를 시작하면 먼저 사용자의 아이디와 권한 속성을 제시하여 서버로부터 인증을 받는다.

step 6. 어플리케이션 서버는 ACL Manager를 호출하여 사용자의 권한을 결정한다.

Ⅱ. 분산 컴퓨팅 네트워크 보안 시스템

2.1 암호화 된 사용자 보안 시스템

암호화 사용자 보안을 위한 기존의 데이터베이스는 접근통제 방법으로 데이터를 보호하였다. 중요한 데이터의 보호를 위하여 적극적이고 강력한 정보보호 메커니즘이

필요하게 되었고, 제안 한 시스템에서는 다음 3가지 기능을 추가로 실현하였다.

a. 암호화 사용자 인증 기능

일반적으로 사용자 인증에 사용되는 비밀번호 기법은 비밀번호 자체가 그대로 시스템 내에 존재하므로, 외부에 노출될 염려가 있어 보안이 취약하다. 이에 암호화 기법을 이용한 사용자 인증 방법으로 제안 시스템에서는 공개키 암호화 방식을 적용하여 아이디와 비밀번호를 암호화하여 저장하였다[그림 4]. 인증시 암호화된 비밀번호를 비교하여 사용자 시스템과 서버 시스템간에 상호 인증을 함으로 보다 강력한 보안을 유지할 수 있고, 정보를 효과적으로 이용 할 수 있도록 하였다.

그림 4. 분산컴퓨팅 환경에서 암호화인증 시스템

Fig. 4. Encrypted user authentication system of distributed computing network

b. 암호화 및 복호화 기능

데이터 보호에 있어서 RSA 암호 알고리즘 방법을 적용하여 아이디와 비밀번호를 암호화해서 저장하므로 허가받지 않은 사용자로부터 정보보호 시스템을 보호할 수 있다. 제안한 암호방식은 암호화된 데이터의 기억장소 크기가 변하지 않고, 또한 RSA 알고리즘을 사용하면 같은 내용을 암호화했을 때 적용된 키 값이 서로 달라 다르게 암호화 되어 나타나 해독이 거의 불가능하다.

c. 데이터베이스와 연결 기능

데이터베이스 사용자가 기존의 DBMS 패키지를 사용하면서 데이터베이스의 보안을 요구하는 부분이 있을 때는 제안시스템의 정보보호 기능을 사용할 수 있다. 본 논문에서 제시한 데이터베이스 연결 모듈과 데이터 암호화 방법과 같이 기존의 데이터베이스와 완전 호환성을 가지고 있으며, 본 논문에서는 사용자 인증 부분의 보안강화 및 비밀 데이터 자체의 암호화 상태유지, 데이터베이스의 보안기능, 데이터베이스 특성 등 질의어를 이용하여 연결할 수 있다.

2.2 암호화 사용자 인증 모듈

암호화 사용자보안 시스템에서 사용자인증은 매우 중요하며, 암호화 기법은 메시지의 전송 및 저장된 데이터를 인증하는데 유용한 수단이 되고 있다. 암호화가 수동적 침해에 대한 보호방법이라면, 인증은 능동적 침해에 대한 보호 방법이다. 이러한 침해로부터 정보를 보호하기 위하여 인증모듈은 정보보호 시스템으로 가기 전에 전처리 모듈로서 공개키 암호방식을 인증시 사용하여 허가자 외에는 사용할 수 없게 강력한 인증모듈을 구성하였다.

a. 암호화 사용자 인증 키 생성 및 관리

암호화 인증 모듈에 사용되는 키는 공개키와 비밀키로 나눌 수 있으며, 정보보호 서버, 시스템을 비롯하여 사용자 시스템 모두가 각각 공개키와 비밀키를 가지고 있다[표 1].

표 1. 인증시 사용되는 키의 종류

Table 1. Type of Key for authentication

사용자	키	함수	보관
User	공개키	(E_k, n)	서버 보관
	비밀키	(D_k, n)	사용자 보관
Server	공개키	(E_k, n)	서버 보관
	비밀키	(D_k, n)	서버 보관
Group	공개키	(E_k, n)	서버 보관
	비밀키	(D_k, n)	그룹구성원 보관

키 생성 및 관리에 있어서 공개키는 모두 서버시스템에서 관리 · 보호하고 있다가 필요시에만 허용하여 준다. 공개키라 하더라도 누구에게나 함부로 공개되지 않으며, 정보보호 서버 시스템에서 공개되었다 하더라도 암호화가 되어 있기 때문에 본인 이외는 아무도 알 수가 없다.

b. 암호화 사용자 인증 파일 생성

다수의 사용자가 정보보호 서버에 접근함에 있어서 정당성 여부, 자료의 불법적 사용, 데이터 파일의 불법적 변경 및 합법적 도용 등을 방지할 수 있는 암호화 인증 시스템을 설계하였다. 일반적으로 정보보호 서버 시스템 인증을 위한 파일 구성은 다음과 같다[표 2].

표 2. 사용자 인증 파일

Table 2. User authentication file

아이디	비밀번호
user01	1234
user02	4567
user03	7890
user04	0123

일반적으로 인증 과정은 아이디와 비밀번호를 입력받아 같으면 인증이 되지만, 본 논문에서는 아이디와 비밀

번호를 인증파일 생성시 다음과 같이 암호화하여 저장하여 두고 인증시 RSA 암호 알고리즘을 이용하여 확인한다. 암호화 인증 파일의 생성 및 등록 절차는 다음과 같다.

step 1. 소수 생성 프로그램을 이용하여 적당한 자리의 소수를 생성한다.

step 2. 두 개 이상의 자리수가 서로 다른 소수 p, q를 선택하여 $p-1$, $q-1$은 큰 소인수를 갖고, gcd $(p-1, q-1)$는 작은 것을 선택한다.

step 3. 모듈러 $n=p, q$를 계산하고 lcm $(p-1, q-1)$보다 작은 E_k(공개키)를 선택한다.

step 4. Euler 함수인 $\phi(n)=(p-1)(q-1)$를 계산하고, Euclid 알고리즘을 이용하여 E_k의 역 모듈러 $\phi(n)$을 계산하여 (3)에서 선택한 키 E_k에 쌍이 되는 비밀키 D_k를 정한다.

step 5. 두 개의 키를 비밀키 D_k와 공개키 E_k로 한다.

step 6. 사용자 등록 테이블에서 사용자 이름을 기본키로 사용하고, 비밀번호의 값을 서버의 암호화 키로 암호화하여 저장한다.

step 7. 아이디와 비밀번호는 암호화되어 파일 에 저장되며, 인증파일을 생성 후 사용된 p, q, E_k를 삭제하고 D_k는 개인이 보관한 후 종료한다.

예를 들어 사용자 이름이 "user01"이고 비밀번호를 "1234"라고 하면, 소수 $p=2029$, $q=7793$을 선택하고, D_k값을 1886827로 하면n=p×q=2029*7793=1581997이고, $\varphi(n)$= (p-1)(q-1)=2028*7792=15802176 이 된다. 여기서 $\phi(n)$, E_k를 Eucild 알고리즘을 이용하여 $D_k=1886827$를 구할 수 있다. 위와 같은 초기값을 가지고 인증 파일에 등록하면 다음과 같다[표 3].

표 3. 사용자 인증 파일의 초기값
Table 3. Initial value of user authentication file

아이디	비밀번호	E_k	D_k
user01	1234	67	1886827
user02	4567	17	7133489
user03	7890	79	1401271
user04	0123	61	17853541
n	q	p	
15811997	2029	7793	
13483693	1789	7537	
8521307	3743	2549	
21791339	6829	3191	

등록될 비밀번호 암호화 값은 서버시스템의 공개키와 자신의 개인 비밀키로 두 번 암호화 하여 얻은 67의 값을 [표 4]와 같이 저장한다. 아이디와 비밀번호는 암호화되어 파일에 저장되며, 인증 파일의 생성 후 p, q, D_k 는 삭제하고 E_k는 개인이 간직한다.

표 4. 사용자 인증 파일
Table 4. User authentication file

아이디	비밀번호	E_k	n
user01	1234	67	15811997
user02	4567	17	13483693
user03	7890	79	8521307
user04	0123	61	21791339

c. 암호화 사용자인증 절차

사용자인증을 받은 사용자가 자원을 사용하기 위해서는 인증모듈을 거쳐야 사용할 수 있다. 제안 시스템의 인증절차는 데이터베이스에 대한 보호 모듈로 암호화된 아이디와 비밀번호를 입력받아 비밀키를 이용하고, 인증모듈을 통하여 데이터베이스의 사용자인증 여부와 권한을 부여 받는다. 암호화 사용자인증 절차는 [그림 5]와 같다.

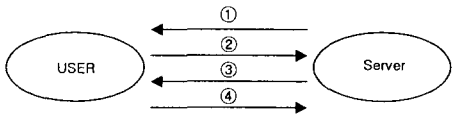


그림 5. 암호화 사용자인증절차
Fig. 5. Process of encrypted user authentication

step 1. 사용자 아이디와 비밀번호를 암호화 $(D_U(E_S(ID, Password, D_u)))$하여 서버에 보낸다.

step 2. 서버는 사용자 인증 파일의 내용과 비밀번호를 암호화하여 보내온 아이디와 비밀번호를 비교하여 비밀번호가 같으면, 메시지를 암호화 $(D_S(E_K(m)))$하여 사용자에게 보낸다.

step 3. 사용자는 보내온 암호문을 복호화 $(E_S(D_K(C))$하여 서버에게 보낸다.

step 4. 서버는 보낸 메시지와 같은 내용의 응답이 오면 사용자의 인증을 부여한다.

2.3. 데이터베이스 연결 모듈

a. 암호화 데이터베이스 생성

데이터베이스 생성은 기존의 데이터베이스를 그대로 사용하기 때문에 암호화하여 할 애트리뷰트의 구조를 바꾸어야 한다. 암호화 하고자 하는 애트리뷰트가 숫자이거나 문자면 모두 문자형태로 구조를 바꾸어야 한다. 암호화 과정을 거치면 모두 문자형태로 바뀌기 때문이다. 회원가입 테이블에 대한 변환과정은 [표 5], [표 6]과 같이 연결된다.

표 5. 회원가입 테이블 구조
Table 5. Table structure

성명	아이디	비밀번호	주민등록번호
Name	id	password	juminno
X(10)	X(8)	X(8)	X(15)
성별	직업	E-mail	
sex	job	email	
X(1)	X(10)	X(15)	

표 6. 암호화 회원가입 테이블 구조
Table 6. Encrypted table structure

chk	Name	chk	id	chk	password	chk	juminno
9	X(10)	9	X(8)	9	X(8)	9	X(15)
성별		직업		E-mail			
chk	sex	chk	job	chk	email		
9	X(1)	9	X(10)	9	X(15)		

[표 6]에서 암호화 애트리뷰트가 숫자인지 문자인지 구분하기 위해 체크 바이트한 바이트를 준다. 숫자를 암호화 하면 문자가 되므로 복호화 시를 생각하여 구분하여야 한다.

b. 암호화 데이터베이스 복호화

데이터베이스 사용은 사용자의 입장에서 보면 다를 것이 없으며, 단지 체크 바이트를 구분하여 0이면 그대로, 1이면 문자의 복호화 이고, 2이면 문자를 복호화 하여 숫자로 변환된다.

Ⅲ. 암호화된 사용자 보안 시스템

제안 시스템은 독립성과 보안이 유지되고 보편적이며, 또한 사용자에 대한 인증과 데이터베이스에 응용하기 쉽도록 설계되어 있다. 또한 사용자가 명령문 수행 중 허가받지 않은 사용자가 접근을 하더라도 정보를 이용 할 수 없게 하였다. 데이터 저장을 위한 물리적 구조는 한 논리 레코드가 임의의 물리적 블록에 저장될 수 있도록 설계되어 있으며, 사용자 인증 테이블은 기본키로 사용자 아이디와 비밀 번호를 암호화 하여 저장하는 테이블로 구성되었다[표 7].

표 7. 사용자 인증 테이블 구조
Table 7. User authentication table structure

아이디	비밀번호	공개키
user01	1234	67
user02	4567	17
user03	7890	79
user04	0123	61

사용자 아이디는 사용자 테이블의 기본키이고 사용자가 데이터 베이스를 사용하려면 사용자 아이디와 비밀번호, 개인키와 서버시스템의 공개키로 비밀번호를 암호화하여 사용자인증 테이블과 비교하여 인증이 확인되면 정보를 이용하고, 인증이 확인되지 않으면 정보를 이용할 수 없다.

Ⅳ. 암호화 사용자보안 시스템의 안정성

정보보호 키 분배 시스템은 허가 받지 않은 불법 사용자에 의한 고의적인 방해와 공격을 막기 위하여 사용자 시스템과 정보보호 서버간의 상호인증 방식을 적용하였다. 상호인증 작업은 Kerberos의 인증시스템을 기반으로 정보보호 시스템을 구성하고 있는 사용자들이 자신의 서비스 코드의 등록과 요구 등의 작업을 수행할 때 해당 사용자가 적법한 사용자인지를 식별하기 위해 수행된다. 이를 위하여 전체 사용자의 대칭키를 분배하기 위해 정보보호 키 분배 센터를 구축하였고 각 사용자들은 정보보호 키 분배센터의 인증을 통한 키 분배방식과 제공된 대칭키를 기반으로 암호화된 패킷을 전송한다. 따라서, 각 사용

자와 정보보호 서버간에 전송되는 암호화된 패킷들은 허가받지 않은 불법 사용자가 해독하거나 변조된 메시지를 통한 정보의 유출을 방지할 수 있었다.

암호화 사용자보안은 적극적인 정보보호 대책의 일환으로 단순하면서도 강력한 보안 방법으로 사용자 인증시에는 단순한 비밀번호 방식을 지향한 RSA 암호 알고리즘을 적용하여 사용자의 신분확인을 안전하게 하였고, 신분확인 후 자원에 대한 보호를 단계적으로 적용할 수 있도록 구현하였다.

또한, 암호화 사용자 인증 알고리즘은 RSA 공개키 암호방식을 기반으로 하여 이산대수 문제 및 합성수의 소인수 분해 문제를 이용하여 정보보호 시스템의 안전성 및 효율성의 비중에 따라 정보통신망의 환경에 적합하며, 사용하기에 편리한 것으로 나타났다. 그러나, 시스템의 성능을 고려할 때 키 분배 과정은 공개키 암호방식을 이용하여 초기의 세션키를 공유한 뒤 비밀키 암호 방식을 사용하는 것이 일반적이다. 따라서 본 논문에서 제안한 정보보호 키 분배 방식은 이산대수 문제 및 합성수의 소인수 분해 문제의 어려움에 기반을 둔 안전한 키 분배 방식이라 할 수 있다.

V. 결 론

본 논문에서는 접근통제기법, 사용자 인증기법, 침입탐지기법을 기술하고, 최종적으로 이를 기반으로 허가 받지 않은 사용자로부터 암호화 데이터베이스를 보호하기 위한 시스템을 설계해 보았다. 제안한 암호화 사용자 보안 시스템은 암호 해독자가 암호문의 정보를 탈취하였더라도 평문으로 해독할 수 없는 기밀성이 보장되며, 안전하게 정보를 보호할 수 있었다. 또한 암호화 사용자 보안 시스템에서는 사용자 시스템과 서버시스템간의 상호 인증 작업을 위하여 시스템간의 대칭키를 분배하기 위하여 정보보호 키 분배 센터를 구축하였다. 이는 사용자 보안 시스템 간에 주고 받는 암호화 패킷들은 허가받지 않은 사용자에게 의해 해독되거나 변조된 메시지를 통한 정보의 유출을 방지할 수 있었다. 정보보호 키 분배 시스템을 이용한 암호화 사용자 보안 시스템은 기존의 사용자 보안 시스템을 보완한 방법으로 단순한 비밀번호 방식을 지향한 RSA 공개키 암호방식을 적용하여 암호화 인증 절차를 설계하였다. 암호화 사용자 보안은 사용자의 신분 확인을 안전하게 하였고, 신분확인 후 자원에 대한 보호를 단계적으로 적용할 수 있어 접근 통제에 효율적이었다.

참고문헌

[1] George Coulouris. Jean Dollimore and Tim Kindberg. "Distributed Systems Concepts and Design". *Addison-Wesley* Publishing Company. 1994

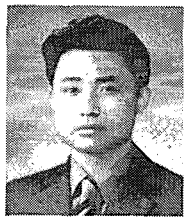
[2] Sung-Ki Yang, "User Authentication System using RSA Algorithm". *ITC-CSCC 2002*, The 2002 International Technical Conference on Circuit/Systems, Computers and Communications, vol. 1. pp.156~159, 2002

[3] D.Y. Lee, B.S Bae, S.J Wi, J.P Jeong, S.J Lim. "Encrypted database security construction for information protection in distribute computing environment". *SAM'03* International Conference, vol. 2. pp.631~635, 2003

[4] 한국정보보호진흥원, 『정보보호 기술교육과정(암호이론/암호응용기술)』, 2001.

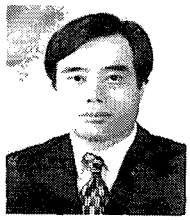
[5] 김기현, "접근통제기술개요", 한국정보보호진흥원, 1999

저자소개



이 대 영(Lee Dae-Young)

1993.3~1999.2 조선대학교 학사
1999.3~2001.2 조선대학교 전산통계학과 석사
2002.3~2006.2 조선대학교 전산통계학과 박사
※ 관심분야 : MANET protocol, 유무선 네트워크 보안, 유비쿼터스 컴퓨팅



김 옥 환(Kim Ok-Hwan)

2000.3.~2002.8 전남대학교 전자공학과 석사
2003.3~2005.8 목포해양대학교 박사수료
1991.6.1~1994.10.31 해양수산부 목포지방 해운항만청
1994.11.1~2005.3.31 (주)CMB웹앤티비 방송부장
1999.8~현재 남부대학교 겸임교수
2006.3~현재 (주)브로드콤 대표이사
※ 관심분야 : 해상이동통신, 정보통신 일반, 정보통신 행정 및 정책