제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

SMA를 이용한 사용자 정보의 암호화 시스템 설계 및 구현

서 복 진, 정 화 영
예원대학교 정보,경영학부

The Design and Implementation of a Security System of User Information using SAM

Bok-Jin Seo, Hwa-Young Jeong
School of Information and Management, Yewon Univ.

요 약

정보의 편리성 및 효용성에 따라 점차적으로 생활의 일부가 되었으며, 이에 따라 타인의 정보에 접근하여 악용하는 피해사례가 늘고 있다. 따라서, 인증되지 않은 외부 침입자로부터 시스템의 정보보호를 위한 많은 노력과 연구가 병행되어왔다. 즉, 침입탐지 시스템 및 암호화, 복호화 알고리즘을 적용하여 소프트웨어 측면에서의 보안기법과 방호벽 등의 하드웨어적인 보안기술이 도입 및 실용화 되고있는 것이다. 그러나, 이를 적용하기 위해서는 많은 전문적인 지식과 기술이 필요하여 일반적으로 쉽게 적용하기 어렵다.

따라서, 본 논문은 간단히 사용자의 정보를 변형함으로서 사용자정보를 갖는 데이터베이스가 노출되어도 이를 보호할 수 있도록 하였다. 즉, 정보 보호 방안으로 내부적 안전을 위한 프로그램적 기법으로 데이터를 저장할 때 중요한 자료들 데이터베이스 혹은 Mapping Array에 보관된 임의의 암호화 코트를 이용하여 암호화하여 저장하고 필요할 때 복호화 하는 시스템 내부적인 보안 방법을 제시하고자 한다.

1. 서론

최근 인터넷과 같은 컴퓨터 네트워크 기술이 발전함에 따라 민간이나 정부 분야에서 전자적 거래(Electronic transaction)가 급증하고 있다. 컴퓨터 네트워크를 통한 원격지간의 비 대면 거래방식은 시대가 바뀜에 따라 피할 수 없는 현실이 되었으며,[1] 특히 인터넷의 확장으로 인한 외부인의 시스템 불법침입, 중요정보의 유출 및 변경·훼손·불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등 역기능들이 날로 증대되어 피해규모가 심각한 수준에 이르고 있다. 특히 컴퓨터 시스템의 침해사고가 국내·외에서 빈번히 일어나고 있는 지금 이에 대한 대응책이 어느 때 보다 절실히 요구되고 있다.[2]

현재 수많은 암호화 방식이 소개되고 또 개발되고 있다. 이러한 수많은 암호화 알고리즘의 적용은 많은 문제점이 야기한다. 업무의 특성상 복잡한 처리, 많은 처리시간의 소요 초조자의 사용에 있어 어려움과 경비의 부담 등 암호화 알고리즘의 적용 문제점이 많다.

따라서, 본 논문에서는 안전한 정보보호를 위하여 mapping array를 이용한 사용자 정보보호 시스템을 제시하고자 한다. 이는, 사용자의 정보를 데이터 베이스에 보관함에 있어 mapping array의 값을 임의적으로 참조해 암호화함으로써 사용자의 아이디와 비밀번호, E-mail등의 도용 및 노출을 최대한 방지하는 암호화 시스템을 설계 및 개발하였다.

2. 암호화 방식

암호화는 자료의 기밀성을 보장하는 방법이다. 암호화는 일반적으로 원래의 자료와 그것을 암호화하는 키와 암호화된 자료와 그 암호화된 자료를 원래의 자료로 복원시키는 키 등으로 구성된다. 암호화 방식에는 수많은 내용이 소개되고 개발되고 있다. 이에는 대칭형 암호화 방식 또는 비밀키 암호화 방식(Symmetric Secret Key Cryptography)과 비대칭형 암호화 방식 또는 공개키 암호화 방식(Public Key Cryptography)이 있다. 이에 관하여, 다음의 <표 1>은 비밀키와 공개키의 암호화 방법을 비교하여 도표화하였다[6].

<표 1> 공개키와 비밀키의 비교

특징	비밀키	공개키
키의수	단일키	한쌍의키
키의 형태	키는 비밀	하나는 공개 하나는 비공개
키관리	단순하나 관리에 어려움	디지털 증명과 신뢰할 수 있는 제3자가 필요
속도 (상대)	매우 빠르다	느리다
용도	큰 데이터 암호화에 사용	작은 문서의 암호화 혹은 메시지 서명을 하기 위한 Application에사용

2.1 비밀키(대칭형) 암호화방식

대칭형 암호화 방식은 자료를 암호화하는 키와 암호화된 자료를 복호화하는 키가 동일한 암호화 방식이다. 이 방식의 장점은 암호화와 복호화가 빠르고, 여러 가지 다양한 암호화 기법이 개발되어 있다는 점이다. 단점은 복수의 사용자가 동일한 자료를 사용할 때 키의 공유문제가 발생한다.

특징
- 송신자와 수신자 사이의 동일한 키 사용
- 상호간의 신뢰성이 내포
- 키 누출 시 모든 문서에 대한 암호화 가능
- 대규모 사용자를 대상으로한 비즈니스 업무에 부적합

대칭형 암호화 방식으로 DES(Data Encryption Standard), 3DES(Triple DES), FEAL(Fast Data Encipherment Algorithm), IDEA, RC2와 RC4, SKIPJACT들이 이용되고 있다.

대칭형 암호화 방식의 대표적인 것으로는 DES (Data Encryption Standard)방식이 있다. 이것은 미국 상무성의 국립표준국(NBS)에서 미국 표준 암호 알고리즘으로 채택한 64비트 블록의 입력 및 출력을 가지는 64비트 블록 암호이다. 64비트의 키 블록(key block) 중 56비트가 암호화 및 복호화에 사용되고, 나머지 8비트는 키 블록의 parity check 용으로 사용된다.

최근 들어 "DES 알고리즘은 보안성이 깨졌기 때문에 통신 보안기술로 사용하지 말아야 한다"는 주장도 나오고 있으나 이는 사실과 다르다. DES에 대한 공격은 천문학적인 반복계산에 의해 가능하기 때문에 현재 공격을 위한 비용이 약 1백만 달러에 가깝다. DES의 보안성을 유지하려면 난수발생 등의 방법을 이용해 자주 비밀키 값을 변경하거나, 이중 혹은 삼중 DES 암호화를 하거나, RSA와 같은 비대칭 암호화기술과 적절히 혼합하여 사용해야 한다[4,5].

2.2 공개키(비대칭형) 암호화방식

대칭형 암호화 방식은 암호화 정보를 네트워크상의 상대편에게 보낼 때 키까지 보내야 하는데, 그 키를 보호할 길이 없다는 문제의식에서 공개키(비대칭형)암호화 방식이 개발되었다.

공개키 암호화방식은 공개키와 비밀키가 한 쌍으로 사용하며 송신자는 수신자의 공개키만 알고도 메시지를 암호화하여 송신할 수 있고 수신자는 자신의 비밀키를 이용하여 메시지를 판독할 수 있다.

공개키 암호화에서, 공개키와 개인키는 인증기관에 의해 같은 알고리즘(흔히 RSA라고 알려져 있다)을 사용하여 동시에 만들어진다. 개인키는 요청자에게만 주어지며, 공개키는 모든 사람이 접근할 수 있는 디렉토리에 디지털 인증서의 일부로서 공개된다. 개인키는 절대로 다른 사람과 공유되거나 인터넷을 통해 전송되지 않는다. 사용자는 누군가가 공개 디렉토리에서 찾은 자신의 공개키를 이용해 암호화한 텍스트를 해독하기 위해 개인키를 사용한다.

특징
- 암호화키와 해독키의 분리
- 하나는 공개 , 다른 하나는 비공개
- 인터넷 비즈니스에 적합
- 공개키는 누출되어도 원문 해독불가

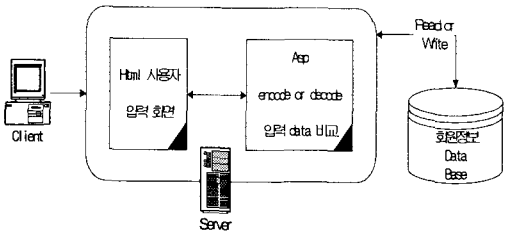
그러므로, 만약 자신이 어느 누구에게 어떤 메시지를 보낸다면, 우선 수신자의 공개키를 중앙 관리자를 통해 찾은 다음, 그 공개키를 사용하여 메시지를 암호화하여 보낸다. 그 메시지를 수신한 사람은, 그것을 자신의 개인키를 이용하여 해독한다. 메시지를 암호화하는 것 외에도, 송신자는 자신의 개인키를 사용하여 디지털 인증서를 암호화하여 함께 보냄으로써, 메시지를 보낸 사람이 틀림없이 송신자 본인이라는 것을 알 수 있게 한다. 대표적인 공개키 알고리즘은 RSA가 있으며 비밀키에 비해 처리시간이 많이 걸린다는 단점이 있으며 키 관리가 효율적인 것이 장점으로 알려져 있다. 복합 암호화방식은 비밀키 암호방식으로 DES방식의 처리시간단축과 RSA의 키 관리를 결합한 방식으로 전자우편 표준인 PEM(Privacy Enhanced Mail)과 PGP(Pretty Good Privacy)를 들 수 있다[3,5,6].

3. SMA(Security Mapping Array)를 이용한 사용자 정보 암호화 시스템

본 논문에서는 외부적 보안보다는 내부적 입장에서의 자료들을 한번 더 안전하게 암호화하여 자료를 보관하여 내부에서 또는 침입이후 자료의 유출에 대비한 보안 시스템의 구현을 위하여 웹기반에서 login 되는 사용자들을 데이터베이스에 보관할 때 배열에 보관되어있는 자료를 이용하여 사용자 id와 password를 암호화하여 저장하는 방식을 구현하였다.

3.1 시스템 구성도

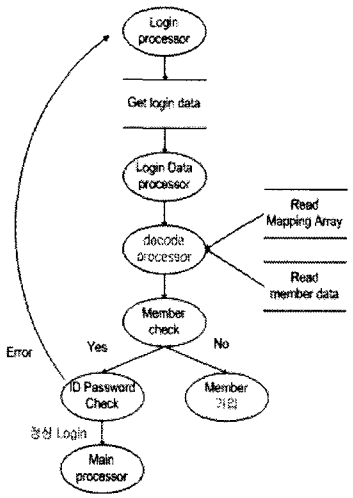
<그림 1>와 같이 client측에서 입력한 자료를 서버 측에서 html 언어로 입력화면을 구성하여 입력받으며 입력받은 자료는 Web Server에서 CGI 언어를 이용하여 Post방식으로 처리하며, 보안을 요하는 자료 값을 Sql Server에 보관된 Mapping Array에서 암호화 값을 읽어들이고 Web Server에서 임의의 난수 값을 발생하여 난수 값으로 암호화하여 다시 Sql Server에 전송하여 보관한다.



<그림 1> 시스템 구성도

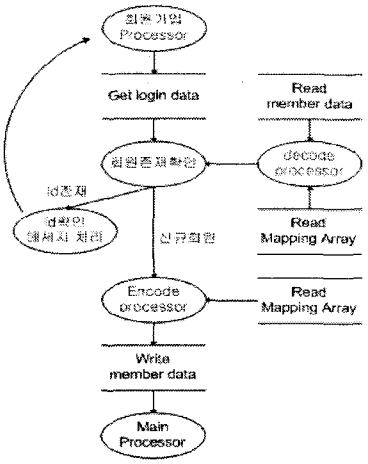
3.2 시스템 설계

본 논문에서는 Mapping Array를 이용한 암호화 방식의 전체적인 프로그램의 흐름을 회원 가입 프로그램에 접목하여 활용하였다. 프로그램의 전체적인 흐름은 사용자 입력루틴(login processor)을 이용하여 입력받은 사용자의 id와 password를 Sql Server에 있는 id와 password를 읽어들여 Sql Server의 Mapping Array를 참조하여 복호화 하고, id와 password를 비교하여 정상적 login을 하도록 하고 비정상적인 login을 한 경우 다시 login 화면으로 이동하는 알고리즘을 DFD로 <그림2>에 표현하였다.



<그림 2> Login Processor

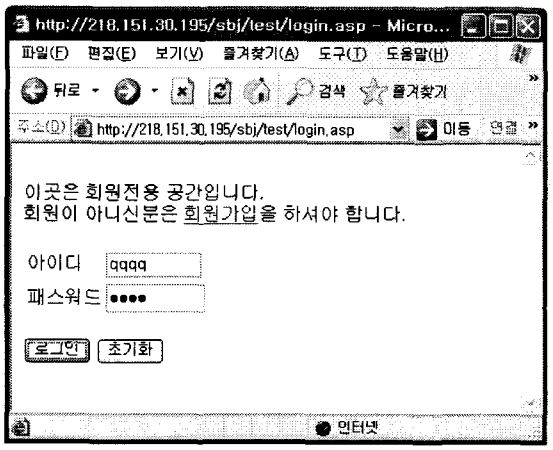
<그림3>은 신규 회원가입자의 경우 알고리즘으로 회원등록 창에서 회원id 와 password를 입력하여 저장하면 id와 password를 SQL Server의 Mapping Array를 참조하여 암호화 하여 SQL Server에 저장하고 Login화면으로 이동하는 알고리즘이다.



<그림 3> 회원등록시의 암호화 과정

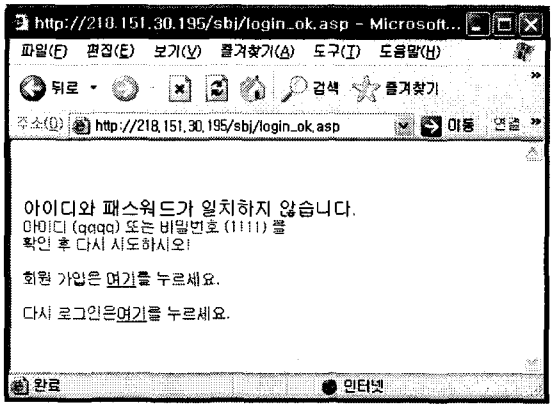
3.3 Mapping Array를 이용한 암호화 시스템 구현

WEB상에서의 화면 구성과 암호화와 복호화 시스템구성은 다음과 같다.



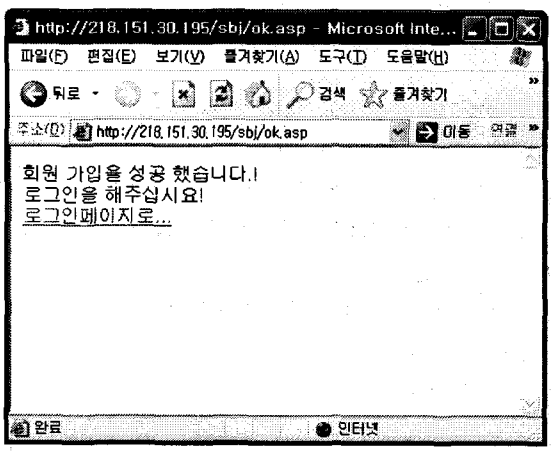
<그림 4> Login 화면

위의<그림4>에서처럼 로그인 화면에서 사용자의 Id와 Password를 입력후 로그인하면 Sql Server에 저장되어있는 Iid와 Password를 읽어들여, Mapping Array를 이용하여 저장되어있는 Id와 Password를 복호화 하여 입력받은 Id와 Password를 비교하여 비정상적인 Login인 경우에는 <그림 5>과 같이 회원가입 혹은 ID 와 Password의 재 입력을 요구한다.



<그림 5> Login 실패시 화면

위의 <그림 4>에서 회원가입을 선택하거나, <그림 5>에서 회원 가입을 선택한 경우에는 <그림 6>과 같이 회원 가입 창이 나타난다.



<그림 6> 회원등록 성공시 화면

회원 가입을 선택했을 때 입력받은 회원의 id와 password를 SMA이용하여 암호화하여 Sql Server에 저장하고 Id와 Password의 암호화와 복호화는 관리자 측에서 따로 저장한 Mapping array을 이용하여 암호화하며, 암호화는 임의의 난수를 발생하여 암호화하고 임의 난수 값은 다시 Sql Server 에 저장하는 방식으로 하였다.

4. 결론

우리가 경험하고 있는 인터넷 세상은 수많은 해커들의 위험이 도사리고 있다. 이에, 각종 침입탐지 기법들이 새롭게 연구되고 있으며 새로운 암호화 기법 역시 연구되고 있다. 그러나 해커들로부터 완벽한 안전을 보장하지 못하기에 사용자들은 두려움에 떨고 있는 입장이다. 본 논문에서 소개한 SMA는 관리자 측에서 간편하고 쉬운 방법으로 자료를 내부 사용자들의 도용 및 해커들의 침입에 의해 소실될 개인의 자료 및 중요한 자료를 암호화하여 보관한다면 최소한의 정보유출을 막을 수 있으리라 생각한다. 단점으로는 자료들의 검색에 있어서 보관 되어있는 데이터의 자료를 일일이 복호화 하여 검색하는 과정에서 속도 부분에서 문제가 발생하나 자료들의 값을 코드화하여 검색자료들의 색인 한다면 이용하여 보관한다면 중요자료의 유출은 방지할 수 있을 것이다. 앞으로 해커들의 침입을 막을 수 있는 획기적인 방안과 대책이 더 많은 연구개발로 마련되어야 할 것이다.

참고문헌

[1] 최영철, 홍기용, 이홍섭 "전자서명법과 전자서명 인증관리체제", 한국정보보호센터 정보과학회지 제 18권 제1호 통권 128호 , 2000. 1. ISSN 1015-9908 P13

[2] 한국정보보호센터, "실시간 네트워크 침입탐지 시스템 개발에 대한 연구", Dec., 1998

[3] 안중호, 박철우 "인터넷과 전자상거래 p217~p223" 홍문사, 2001.

[4] http://home.ewha.ac.kr/~jhkim/972project/bs1/ec4_1_2.html, 2002.

[5] http://www.jawon.net/ec_authority.htm, 2002.

[6] http://mail.pihana.co.kr/PKI.htm, 2002.