웹 기반 사용자 정보 암호화 알고리즘 설계 및 구현

최철림*, 정화영**, 송영재***
제일모직(주)응용개발센터*, 예원예술대학교 전자상거래학과**, 경희대학교 컴퓨터공학과***
ironbeanky@yahoo.co.kr*, jhymichael@empal.com**, yjsong@khu.ac.kr***

Design and Implementation of Web Based User Information Security Algorithm

Cheol-Rim Choi*, Hwa-Young Jeong**, Young-Jae Song***
Application Development Center, Cheil Industries*, Electronic Commerce of Yewon Art University**,
Computer Science of Kyunghee University***

요 약

웹 기반 시스템에서 정보보호 알고리즘은 공개키와 비밀키 방식을 들 수 있다. 그러나, 이러한 방식은 별도의 키관리가 필요하며, 소단위 시스템에 적용하기에는 너무 복잡한 알고리즘 처리가 요구된다. 따라서 본 연구는 소단위 시스템에 적용하기 쉬운 간단한 암호화 알고리즘을 통하여 사용자의 정보를 보호할 수 있는 기법을 제시하였다. 즉, 사용자 정보는 정보 맵핑 테이블 값을 기준으로 코드 변형을 위한 연산방식에 따라 변형하여 암호화 및 복호화 하였으며, 사용자 로그인 시스템을 구현함으로서 쉽게 적용 가능함을 보였다.

1. 서 론

컴퓨터 네트워크 기술이 발전은 산업분야에 전환기를 가져왔다. 그러나, 대부분 익명성의 접속으로 이용되는 상황에서 이를 악용한 많은 피해사례가 급증하고 있다. 즉, 외부인의 시스템 불법침입, 중요정보의 유출 및 변경·훼손·불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등이 날로 증대되어 피해규모가 심각한 수준에 이르고 있다. 컴퓨터 시스템의 침해사고가 국내·외에서 빈번히 일어나고 있으며 그에 대한 대응책이 절실히 요구되고 있다[1]. 정보보호를 위한 기존의 연구는 비인증된 사용자의 침입을 감지하는 침입탐지 모델과 암호화를 통한 정보 보호기법이 있다. 이들 중 암호화 알고리즘은 비밀키와 공개키 방식을 사용하고 있으나, 소단위 시스템에 적용하기 위해서는 너무 복잡한 암호화 및 복호화 단계가 필요할 뿐 아니라 별도의 키관리가 요구된다.

본 연구에서는 소단위 시스템에서 쉽게 적용 가능한 암호화 알고리즘을 제안하였다. 이는, 웹 기반 시스템에서 사용자 정보를 서버의 정보 맵핑 테이블에 의해 변환 및 저장함으로서 서버의 정보 노출시에도 사용자 정보를 보호할 수 있도록 하였다.

2. 정보보호 및 암호화 기법

2.1 침입탐지 모델

침입탐지 모델[3,4] 기반의 분류는 침입탐지 방법에 따라 비정상적인 침입탐지 기법과 오용 침입탐지 기법으로 나뉜다. 침입탐지 모델은 침입탐지 시스템 개발에 있어 요구되는 침입 패턴 분석과 유형별 분류 및 탐지 방법 등을 연구함에 있어 많은 기초 정보들을 제공한다[2,5].

2.2 암호화 기법

암호화 기법은 비밀키 암호화 방식과 공개키 암호화 방식으로 나뉜다.

<표 1> 공개키와 비밀키의 특징비교

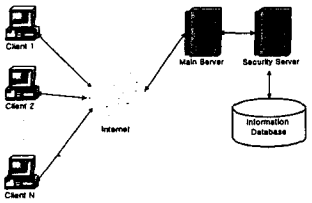
특징	비밀키	공개키
키의수	단일키	한쌍의키
키의 형태	키는 비밀	하나는 공개 하나는 비공개
키관리	단순하나 관리에 어려움	디지털 증명과 신뢰할 수 있는 제3자가 필요
속도	매우 빠르다	느리다
용도	큰 데이터 암호화에 사용	작은 문서의 암호화 혹은 메시지 서명을 하기 위한 Application에사용

비밀키 암호화 방식은 송수신자 둘 다 같은 비밀키를 알고 있어 송신자의 메시지를 비밀키로 암호화하여 보내면 수신자는 비밀키로 복호화 하여 사용한다. 비밀키 암호화 방식은 DES(Data Encryption Standard), 3DES(Triple DES), FEAL (Fast Data Encipherment Algorithm), IDEA, RC2와 RC4, SKIPJACT들이 이용되고 있으며 공개키 암호화방식은 공개키와 비밀키가 한 쌍으로 사용한다. 송신자는 수신자의 공개키만 알면 메시지를 암호화하여 송신할 수 있고 수신자는 자신의 비밀키를 이용하여 메시지를 판독할 수 있다. 대표적인 공개키 알고리즘은 RSA가 있다. <표 1>에서 공개키와 비밀키의 각 특징에 따라 비교하였다. 복합 암호화방식은 비밀키 암호방식으로 DES방식의 처리시간단축과 RSA의 키 관리를 결합한 방식으로 전자우편 표준

인 PEM (Privacy Enhanced Mail)과 PGP(Pretty Good Privacy)를 들 수 있다[6].

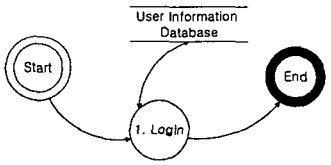
3. 웹 기반 사용자 정보 암호화 알고리즘 설계

본 연구는 공개키를 단순화한 응용 알고리즘이라 할 수 있다. 암호화 대상은 사용자 로그인 ID와 Password로 하였으며 각각 10자리 이하로 제한하였다. 전체적인 시스템구성은 <그림 1>과 같이 메인서버와 인증서버로 나뉘며, 사용자의 로그인 정보는 인증서버에서 암호 및 복호화된다.



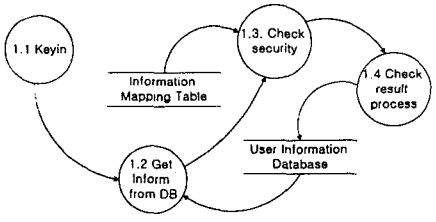
<그림 1> 시스템 구성도

<그림 2>는 사용자 로그인 정보 암호화 자료흐름도의 배경도를 나타낸다. 로그인시의 사용자정보 데이터베이스에는 암호화된 사용자의 ID와 Password만을 가진다. 사용자 로그인 정보의 구체적인 암호화 과정은 <그림 3>과 같다.



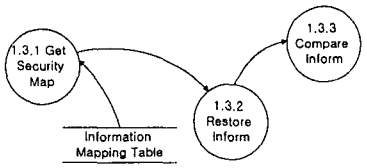
<그림 2> 사용자 로그인 정보 암호화 배경도

1.1의 Keyin 부분은 사용자가 로그인하기 위해서 입력하는 ID와 Password를 가져온다. 1.2에서 사용자의 암호화된 기존의 ID와 Password를 사용자 정보 데이터베이스로부터 가져온다. 1.3에서는 시스템내에서 가지고있는 복호화 맵핑 테이블을 이용하여 데이터베이스로부터 가져온 암호화된 정보를 복호화하며 입력된 정보와 비교하여 정보 인증 여부를 확인한다. 1.4는 인증처리 결과에 따라 인증 및 비인증에 대한 경고처리를 할 수 있다.



<그림 3> 로그인 정보 암호화 자료 흐름도

사용자 정보의 복호화 부분은 <그림 4>와 같다.



<그림 4> 사용자 정보 복호화 및 비교

1.3.1부분은 시스템내에서 배열로 저장된 정보 맵핑 테이블의 배열값을 가져온다. 즉, 시스템내에 다음과 같이 복호화 키가 배열로 저장되어있다.

```
Dim securestr[10]
securestr[0] = "a"
securestr[1] = "0"
    :      :
    :      :
```

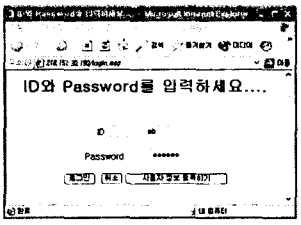
1.3.2부분에서는 배열값들을 적용하여 복호화 과정을 수행한다. 본래의 사용자 ID가 ab라면 <그림 3>의 1.4에서 위 배열값들에 따라 다음과 같이 암호화가 이루어져 저장된다.

a + 0x41(securestr[0]의 ASCII값) = 0x82
b + 0x30(securestr[1]의 ASCII값) = 0x72

따라서, 사용자 정보 데이터베이스로 저장되는 사용자 ID는 0x82, 0x72가 된다. Password도 같은 방법으로 적용되며, 복호화 과정은 이의 역순으로 진행된다. 1.3.3에서는 복호화된 정보와 입력된 정보를 비교하여 인증검사를 한다.

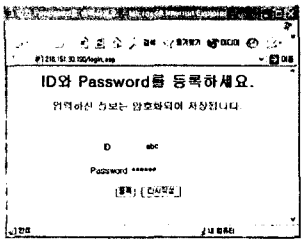
4. 웹 기반 사용자 정보 암호화 알고리즘 구현

본 연구는 Windows XP 환경에서 구현되었으며 ASP와 MS-ACCESS 데이터베이스를 이용하였다. <그림 5>는 로그인 화면을 나타낸다.

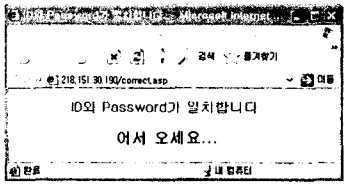


<그림 5> 사용자 로그인 화면

새로운 사용자는 사용자 정보 등록하기에서 <그림 6>과 같이 ID와 Password를 등록할 수 있다. <그림 5>에서 ID와 Password를 입력한 후 로그인을 하면 복호화 과정을 거쳐 사용자정보를 비교하고 일치되었을 경우 <그림 7>과 같은 인증 이후의 화면을 볼 수 있다.

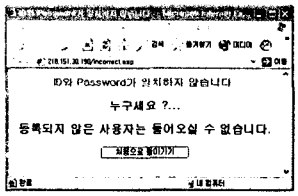


<그림 6> 사용자 정보 등록하기 화면



<그림 7> 인증된 사용자 로그인 이후의 화면

그러나, 사용자의 정보가 일치되지 않은 비인증된 사용자의 경우 <그림 8>과 같은 화면을 나타낸다.



<그림 8> 비인증된 사용자의 경고화면

5. 결과 비교 및 결론

본 연구는 웹 기반 시스템에서 인증되지 않은 사용자들의 정보도용 및 해커들의 침입에 의하여 정보들이 노출되는 상황에서, 간단하고 쉽게 적용할 수 있는 암호화 알고리즘을 통하여 사용자들의 중요한 정보들을 보호하는데 그 목적이 있다. 따라서, 사용자 정보들 중 ID와 Password를 대상으로 암호화 및 복호화를 통한 로그인 시스템을 설계 및 구현하였다. 본 연구의 적용된 결과로는 <표 2>와 같다.

<표 2> 제안기법의 비교 결과

특징	공개키/비밀키	제안기법
키	필요	불필요
키의 형태	공개/비공개	불필요
키관리	관리필요	불필요
속도	빠르다/느리다	빠르다
용도	큰 데이터 또는 작은 문서의 암호화	소단위 시스템에서의 정보변형

사용자 정보는 각 단어별로 시스템내에 배열로 저장되어 있는 정보 맵핑 테이블의 값을 기반으로 암호화 및 복호화 과정을 수행하였다. 본 시스템의 적용결과 쉽고 단순하며 간단히 응용 가능함을 알 수 있으며, 복잡하고 많은 단계의 처리과정이 없어 인증처리의 속도가 매우 빠르다. 또한, 문서의 암호화 과정이 필요 없으며, 서버의 정보에 변형을 주는 방식이므로 클라이언트측의 정보 복호화 과정이 필요 없다. 본 제안기법은 전자결재 시스템 등과 같은 중요한 대단위 시스템에 적용하기는 어렵지만 소단위 시스템이나 간단한 웹 기반 시스템에는 적용가능 할 것이다.

향후 연구과제로서 보다 효율적인 정보보호 알고리즘 적용을 위해서는 정보 암호화 및 복호화 과정을 보다 세분화하고, 정보변경 처리부분에서 다양한 응용기술이 적용되어야한다.

참고문헌

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

[2] 최영철, 홍기용, 이홍섭 "전자서명법과 전자서명 인증관리체제", 한국정보보호센터, 정보과학회지 제 18권 제 1호 통권128호 , 2000. 1.

[3] 김병구, 정태명 "침입탐지 기술의 현황과 전망" 한국정보보호센터 정보과학회지 제 18권 1호 통권 128호, 2000.1.

[4] 전문석, 임요섭, 김덕호, 김종우, "침입탐지 모델 분석 및 설계", 한국정보보호센터, 1996. 12.

[5] 정보통신부, 정보시스템 침해사고 방지기술 개발에 관한 연구, Jan., 1999.

[6] 안중호, 박철우 "인터넷과 전자상거래 p217~p223" 홍문사

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