제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

SMA를 이용한 웹기반 정보보호 시스템 설계 및 구현

서 복 진, 정 화 영
예원대학교 정보,경영학부

Implementation and Development of Web Based Information Security System using SMA

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

요 약

정보화 사회가 도래하고 인터넷과 네트워크기술이 발전함에 따라 전자적 거래 등 원격지간의 비 대면 거래방식은 시대가 바뀜에 따라 피할 수 없는 현실이 되고 있으며, 이에 따른 시스템 불법침입에 의한 사고사례를 우리 주변에서 쉽게 접할 수 있다.

따라서, 인증되지 않은 외부 침입자로부터 시스템의 정보보호를 위한 많은 노력과 연구가 병행되어왔다. 즉, 침입탐지 시스템 및 암호화, 복호화 알고리즘을 적용하여 소프트웨어 측면에서의 보안기법과 Firewall 등의 하드웨어적인 보안기술이 도입 및 실용화 되고있는 것이다.

따라서, 본 논문은 침입 탐지 기법에 관련된 것들과 과 암호화 방식들의 소개 그리고 정보 보호 방안으로 내부적 안전을 위한 프로그램적 기법으로 데이터를 저장할 때 중요한 자료들 데이터베이스 혹은 SMA(Security Mapping Array)에 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].

한국은행에 따르면 올 상반기 인터넷뱅킹·텔레뱅킹 등 전자방식 결제는 하루 평균 121만5,300건 5조8,853억원으로 지난해 같은 기간에 비해 건수는 5.1배, 액수는 4.9배가 각각 늘어났다. 증권시장에서도 상반기 온라인증권약정이 1,591조3,000억원으로 전체 약정(3,132조9,000억원)의 50.8%를 차지, 절반을 넘어섰다. 전자금융거래가 이처럼 급증하고 있음에도 불

구하고 해킹 등을 통해 남의 돈을 빼돌리거나 불법적인 거래를 하는 것을 막는 장치는 미흡하다는 데 있다. 실제로 얼마 전에는 기관투자가 계좌의 비밀번호를 몰래 빼내 불법으로 250억원대의 주식을 거래한 초대형 금융범죄가 발생해 증시 관계자들을 경악하게 했다. 경찰청 사이버테러대응센터에 따르면 지난해 8월부터 올해 3월까지 국제해커들에게 해킹당한 시스템은 우리나라가 2,497개(39%) 로 가장 많았으며미국 801개(12.5%), 중국 413개(6.5%), 타이완 322개(5.0%), 루마니아 285개(4.5%), 인도 242개(3.8%) 등의 순이었다. 보안시스템 강화는 IT와 관련된 모든 영역에서 필수 불가결한 요소다. 이번에 일어난 사상 최대의 금융사고를 계기로 보안시스템이 강화되는 것은 만시지탄(晩時之歎)이지만 그나마 다행이다. 하지만 이것이 완벽할 수는 없다. 궁극적으로는 인간이 이를 어떻게 통제·활용 하느냐에 달려 있기 때문이다. 사이버 범죄를 막기 위해서는 최첨단 시설과 관리자의 효과적 통제, 이용자들의 보안 협조 등이 맞아야 한다[3].

이에 따라, 본 논문에서는 안전한 정보보호를 위하여 SMA 이용한 사용자 정보보호 시스템을 제시하고자 한다. 이는, 사용자의 정보를 데이터 베이스에 보관함에 있어 SMA에 따라 암호화함으로써 사용자의 아이디와 비밀번호의 도용 및 노출을 최대한 방지하는 암호화 시스템을 설계 및 개발하였다.

2. 침입탐지 시스템 및 암호화 기법

2.1 침입탐지 모델

침입탐지 모델 기반의 분류는 침입탐지 방법에 따라 비정상적인 침입탐지 기법과 오용 침입탐지 기법으로 나뉠 수 있으며 <표 1>은 이의 세부 분류를 보인다[1,4,6].

	침입탐지 기법의 종류
비정상적인 침입탐지 기법	통계적인 방법(Statistical Approach)
	특징추출(Feature Selection)
	예측가능한 패턴생성 (Predictive Pattern Generation)
	행위 측정 방식들의 결합 (Anomaly Measures)
	신경망 (Neural Network)
오용침입 탐지기법	조건부 확률(Conditional Probability)
	전문가 시스템 (Expert System)
	상태 전이 분석 (State Transition Analysis)
	모델에 근거한 탐지 (Model-based Detection)
	키-스트로크 관찰(Keystroke Monitoring)
	패턴 매칭(Pattern Match)

<표 2> 침입탐지 모델 기반의 분류

침입탐지 모델은 침입탐지 시스템 개발에 있어 요구되는 침입 패턴 분석과 유형별 분류 및 탐지 방법 등을 연구함에 있어 많은 기초 정보들을 제공한다[1,5].

2.2 암호화 방식

인터넷 암호화 방식에는 수많은 내용이 소개되고 개발되고 있다. 이에는 비밀키 암호화 방식(Symmetric Secret Key Cryptography)과 공개키 암호화 방식(Public Key Cryptography)이 있다.

비밀키 암호화 방식은 송수신자 둘 다 같은 비밀키를 알고 있어 송신자의 메시지를 비밀키로 암호화하여 보내면 수신자는 비밀키로 복호화 하여 사용하는 것으로 장점으로는 속도가 빠르다는 것이나 단점은 키 관리 문제에 있다.

비밀키 암호화 방식으로 DES(Data Encryption Standard), 3DES(Triple DES), FEAL(Fast Data Encipherment Algorithm), IDEA, RC2와 RC4, SKIPJACT등이 이용되고 있으며 공개키 암호화방식은 공개키와 비밀키가 한 쌍으로 사용하며 송신자는 수신자의 공개키만 알고도 메시지를 암호화하여 송신할 수 있고 수신자는 자신의 비밀키를 이용하여 메시지를 판독할 수 있다.

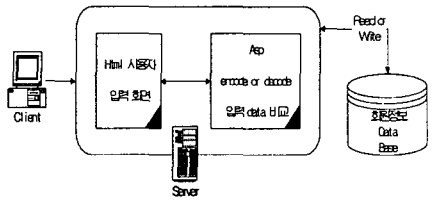
대표적인 공개키 알고리즘은 RSA가 있으며 비밀키에 비해 처리시간이 많이 걸린다는 단점이 있으며 키 관리가 효율적인 것이 장점으로 알려져 있다. 복합 암호화방식은 비밀키 암호방식으로 DES방식의 처리시간단축과 RSA의 키 관리를 결합한 방식으로 전자우편 표준인 PEM(Privacy Enhanced Mail)과 PGP(Pretty Good Privacy)를 들수 있다[7].

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

이처럼 암호화 기법 및 침입탐지에 관련된 많은 기술들이 개발되었고 또 지금도 개발되고 있다 하지만 해킹에 대한 불안감은 해소할 수 없는 것이 우리의 입장이다. 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

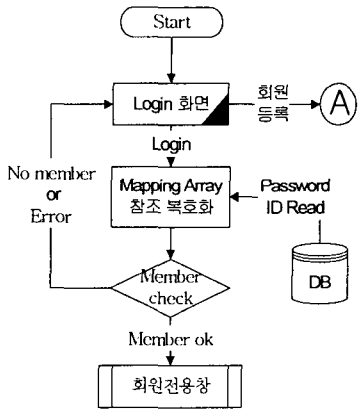
전체적인 시스템구성은 <그림 1>와 같이 client측에서 입력한 자료를 서버 측에서 html 언어로 입력화면을 구성하여 입력받으며 입력받은 자료는 windows2000 server에서 asp언어를 이용하여 post방식으로 처리하며, 보안을 요하는 자료 값을 sql server에 보관된 SMA에서 암호화 값을 읽어들이고 windows2000 servr에서 임의의 난수 값을 발생하여 난수 값으로 암호화하여 다시 sql server에 전송하여 보관한다.



<그림 1> 시스템 구성도

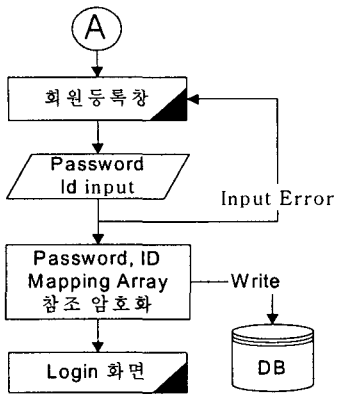
3.2 시스템 설계

본 논문에서는 SMA암호화 방식의 전체적인 프로그램의 흐름을 회원 가입 프로그램에 접목하여 활용하였다. 프로그램의 전체적인 흐름은 사용자 입력 화면(login화면)을 이용하여 입력받은 사용자의 id와 password를 sql server의 Mapping Array를 참조하여 sql server에 있는 id와 password를 읽어들여 복호화 하고, id와 password를 비교하여 정상적 login을 하도복하고 비정상적인 login을 한 경우 다시 login 화면으로 이동하는 알고리즘이다.



<그림 2> SMA를 이용한 암호화 과정

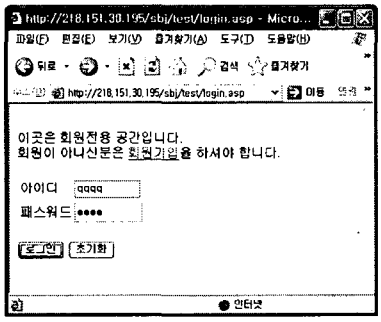
다음 <그림3>의 순서도는 신규 회원가입자의 경우 알고리즘으로 회원등록창에서 회원id 와 password를 입력하여 저장하면 id와 password를 sql server의 SMA를 참조하여 암호화하여 sql server에 저장하고 login화면으로 이동하는 알고리즘이다.



<그림 3 > 회원등록시의 암호화 과정

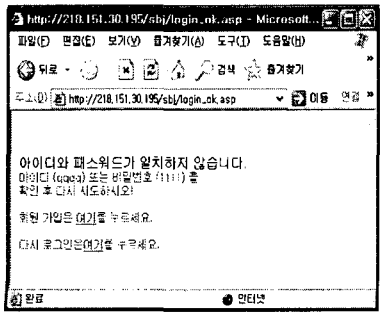
3.3 SMA를 이용한 암호화 시스템 구현

WEB상에서의 화면 구성과 암호화와 복호화 시스템구성은 다음과 같다.



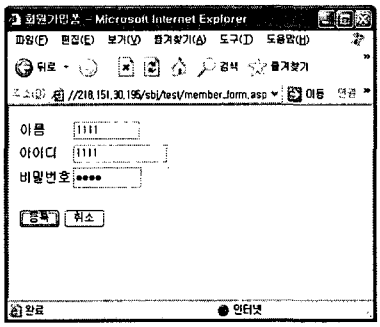
<그림 4> Login 화면

위의<그림4>에서처럼 로그인 화면에서 사용자의 id와 password를 입력후 로그인하면 sql 서버에 저장되어있는 id와 password를 읽어들여, SMA를 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.

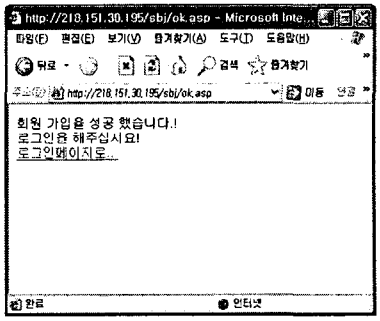


<그림 5> Login 실패시 화면

위의 <그림 4>에서 회원가입을 선택하거나, <그림 5>에서 회원 가입을 선택한 경우에는 <그림 6>과 같이 회원 가입 창이 나타나며 회원 가입을 선택했을 때 입력받은 회원의 id와 password를 SMA이용하여 암호화하여 데이터 베이스에 저장하고 <그림 7>과 같이 로그인 화면으로 이동 메시지를 나타낸다.

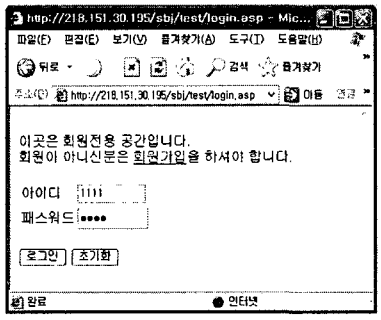


<그림 6> 회원가입창



<그림 7> 회원등록 성공시 화면

<그림 8>에서처럼 정상적인 login인 경우에는 회원 전용화면으로 이동한다.



<그림 8 > 로그인화면

id와 password의 암호화와 복호화는 관리자 측에서 따로 저장한 데이터 맵을 이용하여 암호화하며, 암호화는 임의의 난수를 발생하여 암호화하고 임의 난수 값은 다시 새로운 데이터베이스에 저장하는 방식으로 하였다.

4. 결론

우리가 경험하고 있는 인터넷 세상은 수많은 해커들의 위협이 도사리고 있다. 앞에서 언급했듯이 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.

향후 연구과제로는, 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. 또한, 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] 서울경제신문 2002-08-29 http://news.empas.com/show.tsp/20020829n02981/?s=1081&e=1260

[4] 김병구, 정태명 "침입탐지 기술의 현황과 전망" 한국정보보호센터 정보과학회지 제 18권 1호 통권 128호, 2000.1 ISSN 1015-9908 P30

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

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

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