제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

회원 정보 암호화에 관한 연구

안희선[0] 이옥경 오해석
숭실대학교 컴퓨터학과 멀티미디어연구실
aheesun@hanmail.net[0], oklee017@lycos.co.kr oh@computing.ssu.ac.kr

A Study on the Encryption of the member information

Hee-sun An[0] Hae-Seok Oh
Multimedia Lab., Dept. of Computer Science, Soongsil University

요 약

최근 통신의 발달과 함께 그의 역효과로 정보의 유출에 관한 문제가 대두되고 있다. 이를 해결하기 위해 본 논문에서는 데이터를 저장하기 전 중요 데이터에 대해 대칭키, 즉 세션키를 이용하여 암호화를 하고 이 세션키를 비대칭키인 공개키와 개인키를 이용하여 암호화한다. 우선 세션키를 자신의 공개키로 암호화 하여 저장하므로 데이터에 대한 접근을 하기 위해 필요한 세션키를 자신만이 불수 있도록 한다. 그렇게 하므로 데이터 암호화하는 속도를 빠르게 할 수 있고, 세션키를 따로 공개키로 암호화하여 저장하므로 보안성을 강화할 수 있다.

1. 서 론

최근 인터넷의 발달로 많은 정보들을 서로 공유하게 되었다. 이로 인해 정보를 방대해 졌으나 개인의 정보를 다른 사용자가 도용, 위.변조의 문제가 발생하고 있다. 이렇듯, 네트워크의 발전은 사용자를 편리하게도 하지만 컴퓨터 범죄에 쉽게 피해자가 될 수 있는 소지를 가지고 있다. 즉, 컴퓨터와 네트워크에 대한 의존도가 커지면 커질수록 그 부작용 또한 많아지고 있다. 이러한 부작용은 Tapping에 의한 내용 훔쳐가기, 내용의 변조(Modification), 어떤 사실의 부인(Repudiation) 등으로 대별할 수 있다. 이러한 침해를 막기 위해 암호화 방법이 사용된다. 암호화에는 대칭 암호화와 비대칭 암호화로 나누어질 수 있다. 대칭구조는 암호화 복호화가 같은 키를 이용하고, 이는 속도면에서 비대칭키를 이용하는 것보다 우수하다. 반면 분배의 문제가 있어 비대칭키를 이용하게 되는데 비대칭키는 속도면에선 많이 떨어지지만 분배의 편리성 때문에 많이 이용되는 방법 중 하나이다.

본 논문에서는 중요한 데이터를 암호화해서 저장하므로 외부의 위험으로부터 데이터를 보호할 수 있는 방법을 제안한다. 본 논문의 구성은 2 장에서는 암호, 인증 그리고 전자서명에 대한 이론적인 배경을 기술하며, 3 장에서는 중요한 데이터에 대해 외부의 위험으로부터 보호하기 위한 데이터베이스의 암호화를 제안한다. 4 장에서는 본 연구에 대한 결론을 맺고 향후과제를 제시한다.

2. 이론적 배경

2.1 암호(Cryptography)

암호화란 사람이 인식할 수 있는 정보를 어떠한 규칙에 의해서 알아볼 수 없는 형태로 만드는 기법으로 사람이 알아볼 수 있는 형태로 복구가 가능해야 한다. 이것을 복호화라 한다. 안전이 보장되지 않는 환경에 있는 데이터를 안전하게 유지하거나 네트워크를 통해 전송되는 정보를 보호하는 가장 강력한 수단이다.[1] 암호 알고리즘은 크게 대칭키 알고리즘과 비대칭키 알고리즘으로 나뉘어 진다. 대칭키 알고리즘이란 암호화와 복호화에 동일한 키를 사용하는 것을 의미하며, 비대칭키 알고리즘이란 암호화에 사용된 키와 복호화에 사용된 키가 서로 상이한 알고리즘을 의미한다.

대칭키 암호화에는 각 문자를 다른 문자로 바꾸는 대치법, 위치를 바꾸어 매핑하는 치환법, 그리고 가장 많이 사용되는 것은 DES(Data Encryption Standard)가 있다. 컴퓨터 및 통신 분야에서 데이터를 보호하기 위해 전세계적으로 가장 널리 사용하고 있는 암호화 알고리즘으로 64비트의 평문을 입력받아 56비트의 키를 사용하여 64 비트의 암호문을 출력하는 블록 암호화 알고리즘이다. 이중 DES는 1977년에 56비트 암호화 키는 꽤 쓸만했다. 암호화 키를 모르는 상황에서는 암호 분석은 56개나 되는 1와 0의 모든 조합을 다 시도해야만 한다. 이를 풀기위해 사람이 작업을 하면 1000년 이상이 걸리지만 컴퓨터 트랜지스터은 거뜬하게 해냈다. 그러 인해 DES는 더

이상 강력한 암호화 기법이 아니게 되었고 이로 인해 2중DES와 3중 DES가 나오게 되었다. 2중DES는 각각 하나의 DES 키를 가진 두개의 DES 암호를 사용하는 것이다. 따라서 56비트에서 112비트로 두 배 크게 증가하였다. 이런 키 크기의 증가는 DES의 성능을 두 배 이상으로 증가시켰다. 이를 더욱 보강하기 위해 IBM의 DES 개발팀원 Walter Tuchman 는 단지 두개으이 키를 사용하는 대중에 많이 보급된 현재의 3중 DES를 제안하였다. 하지만 이런 대칭키는 공유하는 것은 힘들고, 남들이 알아서는 안되기 때문에 통신을 하기 위해서는 직접 전달하거나 믿을 만한 사람을 통해 전송해야만 했다. 그로 인해 비대칭키 즉, 공개키와 개인키를 이용하게 되었다.

1970년대에 버클리를 졸업한 학생인, Ralph Merkle 은 공개된 라인에서 비밀키를 교환할 수 있도록 하는 시스템을 제안하였는데 이것이 비대칭키 알고리즘의 시초이다. 비대칭키 암호화 시스템은 암호화할 때 사용하는 키(Public Key)와 복호화할 때 사용하는 키(Private Key)를 다르게 생성하여 공개키(Public Key)는 공개하고 개인키(Private Key)만 안전하게 유지하는 방식이다. 그림 1은 비대칭키 알고리즘을 그림으로 나타낸 것이다.

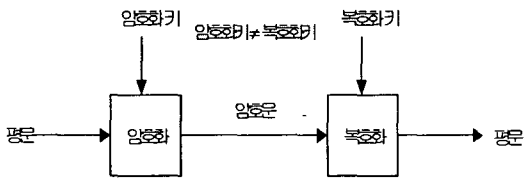

그림 1 비대칭키 알고리즘

RSA 가 대표적인 비대칭키 방식의 알고리즘이다.[2] RSA 알고리즘은 최초로 소개한 3명의 발명자 Ron Rivest, Adi Shamir, Leonard Adleman의 이름을 딴 알고리즘으로 Diffie-Hellman이 할 수 없었던 인증문제를 해결했으며, 키교환 문제까지도 해결하여 지금 시대에 필요한 암호화 시스템으로 자리 잡았다. 이 알고리즘은 두 개의 큰 소수들의 곱과 추가 연산을 통해 하나는 공개키를 구성하고, 또 하나는 개인키를 구성하는데 사용되는 두 세트의 수 체계를 유도하는 작업이 수반된다. 한번 그 키들이 만들어지면, 원래의 소수는 더 이상 중요하지 않으며 버릴 수 있다. 공개 및 개인키 둘 모두는 암호화/복호화를 위해 필요하지만, 오직 개인키의 소유자만이 그것을 알 필요가 있다. RSA 시스템을 사용하면, 개인키는 절대로 인터넷을 통해 보내지지 않는다. 개인키는 공개키에 의해 암호화된 텍스트를 복호화하는데 사용된다. 그러므로, 메시지를 상대방에게 보낸다면, 송신자는 중앙의 관리자로부터 수신자의 공개키를 찾은 다음, 그 공개키를 사용하여 수신자에게 보내는 메시지를 암호화할 수 있다. 수신자는 그것을 받아서, 수신자의 개인키로 그것을 복호화하면 된다. 프라이버시를 확실하게 하기 위해 메시지를 암호화하는 것 외에도, 수신자는 자신의 개인키를 사용하여 디지털 서명을 암호화해서 함께 보냄으로써, 받는 사람 입장에서는 그 메시지가 틀림없이 바로 자신에게서 온 것임을 확신시킬 수 있다.

2.2 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다. 즉, 인증서는 사용자의 공개키가 실제로 사용자의 것임을 증명하는 것이다.[3] PKI에서 인증서의 발행대상은 인증기관, 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다.

인증서의 형식은 1988년 ITU-T가 X.509 초기버전을 공표하고, 1993년에 버전 2를 공표했으며 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동개발되었다. 현재 X.509 버전 3까지 공표되었고, X.509 v3 형식은 다음과 같다.

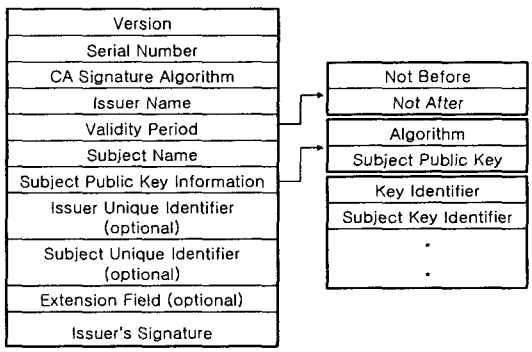

그림 2 X.509 v3

3. 제안하는 정보 암호화

3.1 정보 암호화의 필요성

정보통신망에서 운영되는 정보를 저장 관리하는 컴퓨터 시스템에서 보안(security)의 필요성은 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 판독하거나 또는 부적절하게 기록하는 것을 방지하며, 그리고 정당한 권한을 갖는 사용자의 정보 처리 서비스를 컴퓨터 시스템에서 거부되지 않도록 보호하기 위한 것이다. 특히 대용량의 자료를 보관하는 데이터베이스 관리 시스템에서는 데이터의 무결성(integrity), 기밀성(secrecy), 그리고 확장성(availability) 보장이 필수적으로 요구된다. 따라서 중요한 정보에 대한 보안을 위해 암호화를 이용한 데이터베이스 보안 방법을 제안한다.

3.2 기존의 정보 암호화 기법

정보 유출에 대한 문제가 심각해짐에 따라 많은 업체와 학계에서 정보에 대한 보안에 촉각을 곤두세우고 있다. 이렇게 많은 연구가 되고 있으나 지금까지 제안된 방법은 비대칭 암호화기법을 이용한 공개키로 암호화를 하고, 이를 개인키로 복호화하는 방법이 제안되었다. 그러나 이 방법은 데이터의 양이 증가할수록 많은 시간이 소요되므로 많은 문제점을 가지고 있다. 이를 위해 본 논문에서는 암호화 기법을 비대칭키 암호화를 이용하지 않고, 데이터에 대한 암호화는 대칭키인 세션키를 이용하여 데이터에 대한 암호화 속도를 빠르게 하고, 그 세션키는 비대칭 알고리즘을 이용하여 공개키를 이용하여 암호화 하여 저장하므로 속도면에서와 보안 모두를 향상 시킬수 있는 방법을 제안하였다. 또한 사용자는 기본적으로 ID와 비밀번호만으로 데이터베이스에 접근하는 것을 이 논문에서는 인증서를 사용하여 접근을 할수 있게 한다. 데이터베이스를 관리하는 데이터베이스 관리자는 모든 것에 대해 권한이 있으므로 데이터베이스 관리자를 신뢰할 수 있는지가 중요하다.

3.3 인증서를 이용한 데이터베이스 접근

인증서를 이용한 데이터 보안 방법은 DBA가 발급한 인증서를 가지고 자신의 개인키로 서명을 해서 나온 서명값으로 로그인하고 데이터베이스에 접근할 수 있다. 자신의 데이터를 가져와 자신의 공개키로 암호화하면 다른 사용자뿐만 아니라 데이터베이스 관리자라고 하더라도 볼 수 없다.

그림4는 전체적인 구조는 다음과 같다.

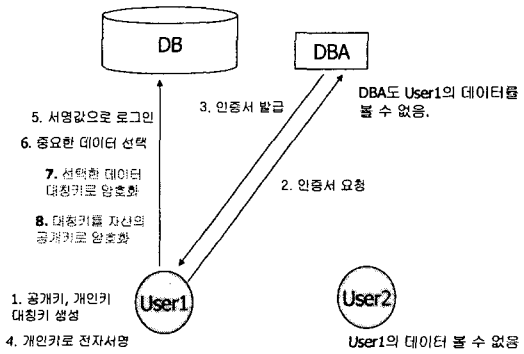

그림 3 제안하는 시스템의 구조

인증서를 이용한 데이터 암호화하는 과정을 설명하면 다음과 같다.

① 사용자1는 공개키, 개인키, 대칭키 생성
② 사용자1의 인증서 요청한다.
③ DBA는 인증서 발급한다.
④ 사용자1는 인증서에 자신의 개인키로 서명을 한다.
⑤ 사용자1는 서명값으로 로그인 한다.
⑥ 중요 데이터를 선택한다.
⑦ 선택된 데이터를 대칭키로 암호화 한다.
⑧ 대칭키를 자신의 공개키로 암호화 한다.
⑨ 복호화는 사용자1의 개인키로만 할 수 있다.

이러한 과정을 거치면 중요한 데이터를 선택적으로 암호화하므로 비대칭키 알고리즘을 이용할 때 보다 속도가 더 빠르고 자신의 개인키로만 복호화할 수 있다.

4. 결론 및 향후 연구과제

데이터 보안이 정보보호 솔루션 시장의 새로운 주역으로 떠오르고 있다. 현재 정보보호 시장의 주역인 네트워크 정보보호 솔루션이 외부의 불법침입에 초점을 맞추고 있는 반면 데이터보안은 기업 내부 사용자의 실수에 의한 데이터 손실을 방지할 수 있어 대규모 데이터베이스를 운영하고 있는 기업이나 금융기관, 인터넷 서비스 업계에서 도입이 확대될 전망이다. 정보보호의 개념이 외부침입에서 내부자 오류

를 방지하는 차원으로 전환되고 있으며 이에 따라 관련 솔루션 시장도 크게 확대되고 있다.

본 논문에서는 인증서를 이용해서 자신의 공개키로 서명을 한다. 그리고 데이터베이스 관리자도 알 수 없는 서명값으로 로그인을 하고 자신의 데이터에 접근할 수 있다. 마지막으로 데이터베이스에 저장할 데이터에 대해서 대칭키로 암호화하고 자신의 공개키로 대칭키를 암호화하면 자신의 개인키로만 복호화할 수 있으므로 다른 사람들은 볼 수 없는 장점이 있다. 또한 선택된 중요한 데이터에 대해 비대칭키 알고리즘이 아닌 대칭키 알고리즘을 사용하므로 속도 또한 빠르다. 기존의 ID/Password로만 데이터베이스에 접근할 때보다 인증서를 사용하고 자신의 개인키로 서명된 값으로 접근하므로 강화된 보안이다. 향후 연구과제는 그룹에서의 데이터베이스 보안에 대한 연구를 할 것이다. 자신만의 데이터를 허가하지 않은 사람의 침입으로부터 보호할 수 있지만 신뢰할 수 있는 사람들에게나 공유할만한 데이터에 대해선 공유할 수 있어야하므로 그룹에 대한 데이터베이스 보안도 필요하다.

5. 참고 문헌

[1] NBS, "Data Encryption Standard", FIPS Pub, 46, U.S, National Bureau of Standard, Washington DC, Jan. 1977.

[2] R. L. Rivest, A. Shrmir, and l. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems." Communications of the ACM, Vol.21, No.2, pp.120-126, Feb. 1978.

[3]Pay Hunt. "PKI and Digital Certification Infrastructure.", IEEE, 2001.

[4] R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", 1978.