정보보안 기술유형 분석

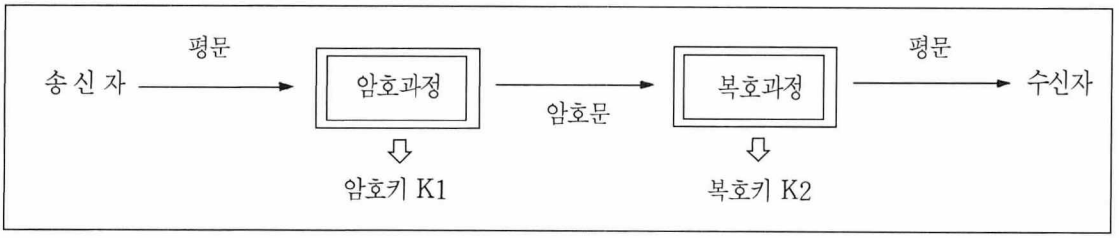
정보화사회가 정착되면서 현재 정부나 민간의 거의 모든 분야에서 다양한 용도로 전산화가 추진되고, 국내외의 각종 통신망을 통하여 수많은 양의 정보를 유통시키고 있다. 이러한 정보통신망 이용의 급격한 증가로 최근에는 정보의 역작용에 대한 정보보안 문제가 새로운 이슈로 떠오르고 있으나, 정보보안을 위한 적절한 대책은 아직 충분하지 못한 실정이다. 보안이 필요한 주요 정보를 각종 정보관련 사고로부터 보호한다는 것은 전산기에 보관되어 있는 상태거나, 보관된 정보의 이동시에 사용자의 과실이나 제3자의 불법행위 혹은 물리적인 자연재해등으로 부터 정보의 안전성을 보장해주는 행위 일체를 말한다. 일반적으로 정보보안이란 물리적인 장애에 의한 정보파괴와 불법적 정보조작등의 모든 장해로부터 정보를 보호하는 것이다. 국방이나 외교적인 측면에서는 물론이고, 최근에는 기업에서도 동종 기업과의 경쟁에서 우위를 확보하고 국제경쟁력을 향상시키기 위하여 정보보안 유지가 반드시 필요한 주요 요소중의 하나이다. 그러므로 컴퓨터와 정보통신망의 확산으로 발생되고 있는 불법적인 정보의 이용, 유출, 파괴,. 등의 정보의 역작용을 억제하기 위한 노력이 시급히 필요하다. 이러한 정보의 역작용에 대한 보안기술로는 물리적 보안기술과 기술적(논리적) 보안기술로 구분할 수 있으며, 주요한 논리적 보안기술의 유형은 다음과 같은 암호시스팀(Cryptosystems), 디지탈서명(Digital Signature), 키 관리(Key Management), 인증(Authentication), 접근제어(Access Control), 및 부인봉쇄(Non-Repudiation)등이 있다.

이 경 석 산업연구원 전산실장

암호화 기술

비인가자가 주요 정보의 사용을 위하여 임의로 패스워드를 도용하거나 액세스 제어시스팀의 통제를 피하여 정보시스팀에 침입하였을 경우, 불법적으로 탈취된 그 정보에 대한 보안을 일정기간 동안 유지시킬 수 있는 마지막 방안은 주요 정보 자체를 암호화시키는 것이다. 이러한 암호기법은 군사나 외교등의 특정 분야에서만 사용되어 왔으나, 최근에는 정보를 취급하는 거의 모든 분야에서 사용하고 있거나 사용을 위한 작업을 진행하고 있다. 현재 정보보호를 위하여 사용되고있는 암호화 기법에는 다음과 같이 비밀키 암호기법과 공개키 암호기법등이 있다.

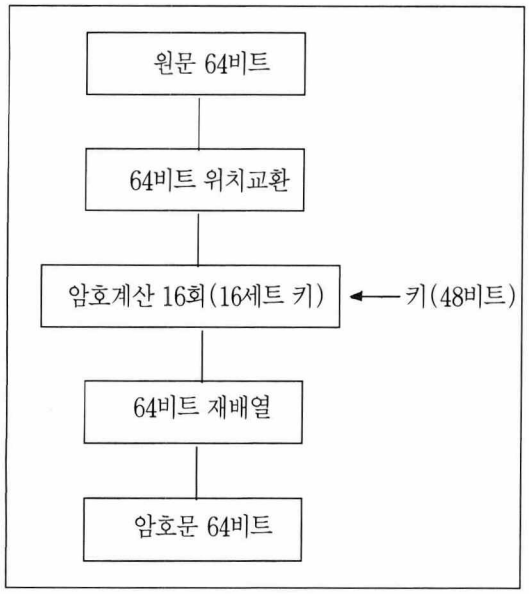
〈 그림 1 〉 암호시스템



1) 비밀키 암호기법 ; 암호화나 복호화시에 하나의 비밀키를 이용하므로 단일키 시스템 혹은 대칭형(symmetric)시스템이라고도 한다. 즉, 〈그림 1〉에서 암호키 K1과 복호키 K2가 같은 경우를 비밀키 암호시스템이라 하며, 정보의 전송을 위하여는 반드시 안전한 경로를 통한 비밀키의 교환이 선행되어야 한다. 이러한 비밀키 시스템의 대표적인 기법이 1977년 미국 상무성 표준국(NBS: National Bureau Standards)에서 정부표준 암호시스템으로 확정한 DES(Data Encryption Standard) 알고리즘이다.

- DES 알고리즘 : 〈그림 2〉와 같이 원문 64비트가 초기배열 과정을 거쳐서 좌우 32비트씩 분리되어 16회의 암호계산을 마친 후 다시 64비트로 모아진다. 그리고 재배열 과정을 끝내면 64비트의 암호문이 생성되는데, 16회의 암호계산시 마다 각각 다른 48비트의 키를 사용한다.

〈 그림 2 〉 DES 알고리즘



- DES 암 복호화 과정 : 첫단계를 제외하고 바로 전 단계의 좌측 32비트가 48비트의 해당키와 XOR 계산을 거쳐 바로 다음단계의 우측 32비트로 되며, 우측 32비트는 그대로 다음단계의 좌측 32비트로 위치한다. 그리고 이처럼 16회의 암호계산을 거친 후 재배열과정을 거쳐 암호과정이 끝나며, 복호과정은 암호과정의 역순으로 이루어지며 16회의 키를 역순으로 적용시켜 암호시와 같은 형태의 과정을 거친다.

2) 공개키 암호기법 : 〈그림 1〉에서 암호키 K1과 보호키 K2가 다른 경우를 말하며, 일반적으로 암호키 K1은 공개한다. 즉, 암호키와 복호키가 상이하여 비대칭형(asymmetric)시스템이라고 하며, 이 시스템은 공개된 암호키에서 합법적인 이용자가 가지고 있는 특정 비밀정보가 없이는 비공개된 복호키를 계산하기가 거의 불가능하다는 특성을 가지고 있다.

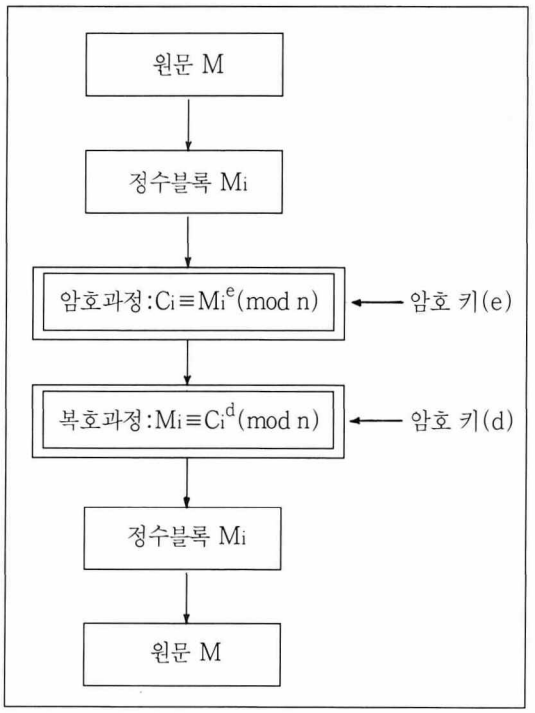
이러한 공개키 암호알고리즘의 기본개념은 1976년 Diffie와 Hellman에 의하여 제안되었으며, 1978년 Rivest, Shamir 및 Adleman등에 의한 RSA 암호시스템과 Merkle과 Hellman에 의한 MH 암호시스템이 각각 공개키 시스템의 실현기법으로 개발되었다.

- RSA 암호알고리즘 : 암호키 e와 복호키 d의 선정을 위하여는, 첫째로 두개의 큰 소수 p 와 q를 구하여 $n=pq$ 및 $\phi(n)=(p-1)(q-1)$을 계산하고, 둘째로 Euler 함수 값인 $\phi(n)$과 서로수 관계를 갖는 공개(암호)키 e를 "$GCD(e, \phi(n))=1$"에 의하여 구하며, 끝으로 공개키 e와 $\phi(n)$을 Euclid 알고리즘에 적용시킨 "$e \cdot d=1 \pmod{\phi(n)}$"의 식에 의하여 비밀(복호)키 d를 계산한다〈그림 3〉.
- RSA 암 복호화 과정 : 원문 M을 일정한 크기의 정수블록으로 변환시킨 Mi에 e승하여 n

으로 나눈 나머지 값인 암호문 Ci(Ci=Mie (mod n))를 만들며, 복호과정은 암호문 Ci에 d승하여 암호과정의 역과정(Mi=Cid (mod n))을 취하게 된다. 그리고 정수블록으로 된 Mi에서 원문상태인 M을 다시 복원시킨다.

- MH 시스팀 : RSA 시스팀은 매우 큰 정수에서 소인수분해의 난이도를 공개키 암호에 응용한 시스팀이고, MH 시스팀은 knapsack 문제의 난이도를 응용하기 위하여 simple knapsack vector와 trapdoor knapsack vector를 최초로 암호에 적용시킨 Knapsack 암호 시스팀이다.

〈 그림 3 〉 RSA 시스팀



디지탈 서명

컴퓨터 통신망을 통하여 송수신 되는 정보인 전자문서에 암호기법을 이용하여 종이문서에 서명하는 것과 같은 기능을 전자적으로 구현하는 것을 디지탈서명이라고 한다.

종이 서류에 의한 문서교환이 통신망을 통한 교환방식으로 대체되므로서 정보의 전달과정에는 상대방의 신분확인, 전달 메시지의 무결성, 사용자의 정당성 및 송수신자간의 분쟁시 해결할 수 있는 조정기능등이 필요하게 되었다.

즉, 전송 메시지가 변형되지 않고 전달되었음을 나타내는 전송 메시지의 무결성과 정보의 생성, 처리, 전송등에 관여한 사용자를 보증하는 사용자 인증등의 양기능을 복합한 것이 디지탈서명이다.

송수신 데이타의 메시지 인증이나 사용자 인증에 사용되는 디지탈서명 과정은 서명이나 검증과정에서 사용할 서명키나 검증키를 만드는 "생성과정"과 디지탈서명 키로 서명자가 비밀정보를 이용하여 메시지를 암호화시키는 "서명과정", 및 공개정보를 이용하여 서명된 메시지가 원래 메시지인지를 확인하는 "검증과정"등이 반드시 필요하다.

1) 디지탈 서명의 요구조건 ; 컴퓨터 통신망을 통하여 안전한 메시지 송수신을 위한 디지탈서명에는 다음과 같은 요구사항들을 만족시켜야 한다.

- 서명자만이 비밀정보로 서명이 가능함.
- 필요시 서명문의 서명자 본인확인 기능이 가능함.
- 서명문에 한번 사용된 서명은 재사용이 불가능함.
- 서명된 내용의 변경이 불가능함(메시지의 무결성).
- 어떤 경우든지 서명자가 서명사실 자체의 부인이 불가능함.
- 분쟁 발생시 제 3자에 의하여 모든 사실과 절차등의 검증과 판정이 가능함.

2) 디지탈서명 방식 ; 신뢰할 수 있는 중재자인 제3자(TTP; Trusted Third Party)의 중재를 통하여 서명을 생성하고 검증하는 "중재자를 통한 서명"과 중재자를 통하지 않고 송신자가 직접 서명하는 "직접서명"등으로 구분된다.

그리고 직접 서명에는 메시지 전체에 대해 서명을 생성하고 검증하며 검증시에 원래의 메시지가 복원되는 "메시지복원형 서명"과 메시지의 해쉬함수 결과에 대해 서명을 생성하고 검증하며 검증시 메시지가 복원되지 않는 "메시지부가형 서명"등이 있으며, 메시지부가형에는 다시 "식별자를 이용한 디지탈서명"과 "확인서를 이용한 디지탈 서명"등으로 분류된다.

그리고 이러한 컴퓨터 통신망에서의 정보보안 서비스 구현에 필수적 기술인 디지탈서명은 메시지처리시스팀(Message Handling System), EDI(Elec-

tronic Data Interchange), 전자자금이체(Electronic Funds Transfer), 화일전송시스팀(File Transfer Systeme), 전자결재(E-mail), 바이러스 체크, 전자선거, 부인봉쇄서비스 (non-repudiation service), 사용자 인증서비스, 데이터 무결성 서비스, 전자화폐,…등에 활용할 수 있다.

키 관리

암호 기술에서 가장 민감한 부분이 암호 키의 관리이며, 암호화된 정보의 보안은 무엇보다도 암호키에 좌우된다. 이러한 키를 관리하는 것은 보안을 유지하는 점에서 볼 때 매우 복잡하고 중요한 요인이다. 키 관리는 키의 생성과 그 키를 사용할 사용자에게 분배하는 문제 및 키의 절취나 파괴등으로 부터의 보호등을 포함한다.

그리고 키를 관리하는 방법은 사용하는 암호시스팀이 대칭형 시스팀이냐 혹은 비대칭형 공개키 시스팀이냐에 따라 매우 다르다.

그리고 정보보안에 사용되는 모든 암호키는 암호의 난이도를 높이고 정보의 안전도를 유지하기 위하여 다음과 같은 이유에서 유효기간이 있다.

- 암호를 공격하는 데는 매우 많은 암호문의 분석이 필요하며, 동일한 암호키로 생성된 암호문이 많으면 많을 수록 암호의 공격에 도움을 준다.
- 주어진 암호키가 쉽게 추측되어 진다거나 암호화나 복호화 과정이 해당키를 암호학적으로 분석할 경우 그키의 수명과 데이타의 안전도에 매우 심각한 피해를 초래한다.

전송되거나 전산기의 저장되어 있는 정보의 보안을 위하여 쓰이는 특정한 키가 암호화에 사용되어지는 기간을 그키의 암호학적 유효기간이라고 하며, 일반적으로 키의 수명은 다음과 같은 요소에 의하여 결정된다.

- 키를 만들거나 키 센타등 특정장소에 등록
- 암호화나 복호화를 위한 키의 분배
- 키의 기능을 부여하는 것과 박탈시키는 비활성화
- 정보유통을 위한 적법한 단사자간의 키의 교환이나 갱신
- 더 이상 암호키로서의 사용을 금지시키는 키의 취소
- 키의 파기와 키의 보관등을 포함한 키의 폐지

접근제어

접근제어(액세스 제어)는 비인가자에 대한 접근을 통제하고, 인가된 사용자에게만 접근할 수 있는 권한을 부여하는 두 가지 기능을 가지고 있으며, 정보의 불법이용과 불법유출을 방지하고, 불법침입자의 위협으로부터 보호하기 위하여 물리적 혹은 논리적인 액세스제어(access control)등의 보안기법이 사용되고 있다.

시스팀내의 데이터 보안성을 유지시키기 위하여는 이용자의 합법성을 인증하여 컴퓨터의 불법이용을 방지하고, 접근권한의 불법취득이나 그 권한과 관련된 각종정보의 불법 변조를 막아야 할 것이다. 그리고 컴퓨터 시스팀에서의 접근제어란 접근을 원하는 이용자가 자신이 합법적인 이용자임을 시스팀에 자신의 신원을 인증시키고, 인증된 이용자가 접근할 수 있는 권한을 확인하는등의 과정을 말한다.

보안이 필요한 정보의 중요도에 따라 비밀등급을 설정하여 이용자가 접근하고자 할 경우, 그 이용자의 비밀취급인가 수준에 따라 접근을 제어할 수 있다. 계층적 분류방식에 의한 외국의 정부나 군 시스팀에서 흔히 쓰이는 보안레벨에는 보안이 필요한 정보는 "Top secret, Secret, Confidential"등의 3가지 레벨로 중요도에 따라 분류한다. 그리고 일반회사나 단체등에서는 "Special control, Company confidential, Private, Internal use only, Information for release, 및 Need-to-know"등을 보안레벨의 강도순으로 사용하기도 한다.

그리고 접근제어 제어의 기본원칙에는 다음과 같이 4가지로 구분할 수 있다.

- 최소한의 권한부여(Least privilege) : 업무수행에 반드시 필요한 최소한의 데이터만을 액세스 할 수 있는 권한을 부여한다.
- 최소한의 노출(Minimal exposure) : 경우에 따라 일부 정보만으로도 관련정보의 액세스가 가능할 경우가 있으므로, 최소한의 데이터만을 노출시켜 불시의 공격이나 고의적인 침투로부터 주요 관련데이터를 보호한다.
- 모든 액세스의 검사(Every access check) :

액세스할 때마다 모든 액세스에 대한 권한을 체크하여 불법침입을 위한 접근을 방지한다.

- 액세스 행위의 검증(Acceptable usage verification) : 액세스 권한 및 정보의 비밀등급 등에 의하여 액세스 행위자체의 정당성 여부를 검증한다.

인 증

인증은 적법한 이용자 여부를 판정하는 첫단계로서 다른 보안기술이나 보안서비스들이 모두 인증에 종속되므로 가장 중요한 보안기술이라고 할 수 있다. 즉, 인증은 개체의 적법성을 검증자에게 보장하여 주며, 인증방법은 다음과 같은 원칙에 기초한다.

- 개체가 자신의 적법성 증명을 위하여 패스워드나 카드 혹은 지문등을 제시
- 제시된 개체의 확인을 위한 판정
- 검증자는 인증과정을 거친 적법한 이용자인 경우에만 개체를 인증

그리고 사용자 개체에 대한 인증은 일방향적이거나 상호적일수 있다. 일방향적 인증은 단지 통신 상대방에 대한 인증이며, 상호인증은 통신 상대방이 서로에 대한 쌍방향 인증이다. 한편, 전산망에서 인증 서비스는 다음과 같이 2가지 환경에 적용된다.

- 개체인증 ; 통신망에 연결된 개체가 적법한 상대인가에 대한 인증
- 원시데이타 인증 ; 발신 데이타가 변조되지 않고 전달되었는가에 대한 인증

그리고 액세스 제어를 위하여 이용자의 신원을 인증하는 방법에는 다음과 같이 3가지 방법이 있다.

- 이용자 지식의 확인법 : 패스워드나 개인고유번호(ID number)등의 확인을 하는 접근제어 기법으로서, 이용자가 시스팀에 접근하고자 할 경우와 시스팀 사용중 특정 데이터의 접근등을 통제하기 위한 기법으로 사용되고 있다.
- 이용자 소유물의 확인법 : 이용자가 소지한 물건(자기카드, IC카드, RF 배지, 스마트카드, …)을 확인하여 접근가능 여부를 판단하는 기법이다.
- 이용자 소유특징의 확인법 : 지문, 망막의 실핏줄, 손의 형태,…등의 이용자 신체 일부분의 특징을 사용하는 생체측정 방법, 그리고 음성, 서명,…등의 이용자의 행위적 특징이나 습관적인 특징을 이용하는 방법등이다.

부인봉쇄

부인봉쇄는 통신내용이나 통신행위 자체를 이용자들이 통신후에 부인하는 것을 방지하기 위한 기술이다. 이러한 기술은 이용자가 자신의 행위를 부인할 수 없도록 하여줄 뿐만 아니라, 통신 상대방 이용자들끼리의 분쟁시 빠르고 정확한 증거를 확보해 줄 수 있는 수단이다. 이런 경우 대부분 믿을 수 있는 제3자의 판정에 의존하며, 정보보안을 위한 부인봉쇄 서비스는 다음과 같다.

- 발신 부인 ; 특정 이용자로부터의 정보발생에 대한 부인이나 정보발생 시간에 대한 불일치등의 발신부인을 봉쇄
- 전달 부인 ; 특정 이용자에게 전달된 정보내용이나 정보의 전달시간등에 대한 불일치등의 발신부인을 봉쇄

그리고 부인봉쇄에는 서비스의 요구, 증거의 확보, 증거의 저장과 전송, 증거의 검증, 및 결과의 검토와 토의 등의 단계가 있다.

결 론

주요 정보의 전송은 컴퓨터와 국내외 통신망을 통하여 언제 어디서나 여러형태의 손쉽게 이용되고 있다. 이렇게 유통되는 정보의 보안에 대한 기술은 종전에 특수분야에서만 필요로 하던 문제였으나, 최근에는 일반 기업이나 각종 기관에서 역시 많은 관심을 갖는 연구분야가 되었다.

불법적인 컴퓨터의 사용, 주요 정보의 변조나 갈취 등에 대한 정보의 역작용으로 부터 안전하게 정보를 보호할 수 있는 암호기술, 디지탈서명, 키관리, 접근제어, 인증 및 부인봉쇄 등의 정보보안기술에 대하여 분석하였다. 이러한 보안기술들이 정보의 피해를 근절시킬 수는 없으나, 정보화사회에서 우려하고 있는 정보의 역작용들을 예방하고 그 피해를 최소화한다든지 혹은 정보범죄의 시도를 억제시킬 수 있는 가장 근본적인 방법이라고 할 수 있다.