데이타 통신 시스템에서의 데이타 보호에 관한 연구

A Study on Data Security in Data Communication Systems

박 충 규 숭전대학교 전기공학과

오 해 석* 숭전대학교 전자계산학과

서 론

컴퓨터 네트워크 시스템이 유행함에 따라 데이타 통신의 량이 크게 증가하게 되었다. 컴퓨터간에 상호 교환하는 데이타의 보호를 위하여 여러가지 기법이 연구되었지만 고의적인 접촉에 대한 완전한 대책이 될수가 없었다. 컴퓨터 네트워크 시스템에서도 일반적인 통신 시스템과 마찬가지로 데이타 암호화에 의한 데이타 보호법이 가장 유효함을 입증하게 되었다. 데이타 암호화라고해서 무전이나, 텔렉스 또는 전자용 방송에서 이용하는 기법과는 다르다. 더욱 고도화된 기법으로 작성된 것이 아니고는 대량의 정보 교환을 필요로 하는 컴퓨터 네트워크 시스템에서는 그 안전을 보증할 수 없다.

본 연구 논문에서, 우리는 먼저 데이타 안전에 위협을 주는 요인들을 알아보고 암호법을 포함한 여러가지의 데이타 보호 방법을 조사하였다. 이어서, 본 연구의 요지인 데이타 암호화에 대하여 기술하였는데 그 과정은 일반적인 암호화 기법과 대조하여 공중 키(Public Key)를 이용한 암호화 기법을 기술하였다.

공중 키(Public Key)자체의 보호에 대하여 연구 기술하였다.

데이타 안전에 대한 위협

중앙 집중 시스템에서의 데이타 안전에에 대한 위협은 여러가지 종류가 있다. 분산 시스템, 즉 컴퓨터 네트워크 시스템에서의 경우는 더욱 많다. 이유는 중앙 시스템에서 일어날 수 있는 위협에 데이타 통신 과정에서 발생하는 위협이 첨가되기 때문이다

본 논문에서는 중앙 집중 시스템에서 공히 발생할 수 있는 위협의 경우는 생략하고 데이타 통신 과정에서 예상되는 위협에 대해서만 기술하기로 한다.

통신 회선상에서의 도청

전용 회선을 이용하는 경우도 물론이고, 통신 회선을 임차해서 사용하는 경우와 인공위성을 통한 회선을 이용하는 경우에 발생할 수 있는 위협의 경우가 도청의 문제이다. 전화의 도청과 같이 데이타 통신 회선의 도청도 매우 간단히 범할 수 있는 방법이므로 데이타 보호의 측면에서 꽤 심각한 문제이다.

허위 데이타의 주입

컴퓨터 네트워크 시스템이 정상 가동되는 과정에서 부정한 허위 데이타를 회선에 주입하는 위협이 있다. 이때, 허위 데이타 주입자는 통신되는 데이타의 패리티 체크(parity check) 사항을 알고 있어서 정당한 데이타의 형식(format)에 모순되지 않게 불량 데이타를 주입하여 통신에 혼란을 야기시킨다.

데이타 보호 방법

배치(batch) 시스템이나 분산지역간의 데이타 통신이 일어나지않는 온라인 시스템에 있어서는 데이타 통신 과정의 위협은 없다. 2장에서 기술한 데이타 안전의 위협요소를

막기 위하여 새로이 연구된 데이타 보호 방법이 데이타의 암호화 이다.

초기의 데이타 암호화는 단일 키(key)에 의한 기법을 사용했었다. 그러나 그 암호시스템을 분쇄하고자하는 고도의 범죄 행위에 의하여, 단일 키(key)를 쉽게 찾아내게 되었고 또 암호화된 데이타는 모두 해독 가능하게 되었다.

단일 키에 의한 암호화에 대하여 알아보고, 그 문제점 및 해결방법을 차례대로 기술해보기로 한다.

단일 키에 의한 암호화 방법

이 방법은 종래의 암호화 방법이라고 표현하기도 한다.

논문의 요지로 기술하고자하는 공중 키(public key)를 이용한 암호화 방법이 연구되기 이전에 사용했던 이 방법은 암호화 방법의 시초이었다. 그림 1에서 보여준 것처럼, 두 노드간에는 키(key) 에 의하여 암호화되고 해독되는 지속의 통신 채널이 형성된다. 전송자인 갑에서 메시지(또는 데이타) 을 수신자들에게 전송하기 전에 먼저 키(key) 에 의하여 암호화 한다.

프레인텍스트(plaintext) (그림에서 M) 가 암호기를 통과하면 사이퍼텍스트(ciphertext) (그림에서 M^K) 가 되어 을에게 전송되며 을의 노드에서는 해독기에 의하여 자동 해독된다. 즉, M^K 가 해독기에 의하여 해독될 때 키(key) K 가 관여하고 그 결과는 다시 프레인텍스트(plaintext) M 가 되어 을에게 전달된다.

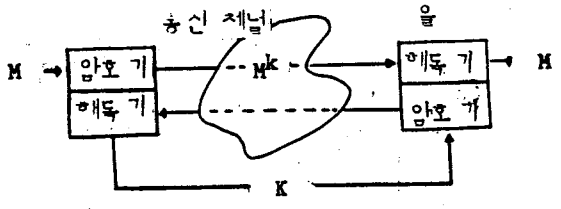

그림1. 단일키에 의한 암호화

이 방법에서 사용하는 키(key) 는 (갑) 과 (을)에게 공동으로 사용된다. 이유때문에 이 방법을 대칭 암호화법(Symmetric encryption method)이라 불리어지기도 한다. (SIMM 79.

이 방법에서 키(key) 에 대한 비밀만 지켜진다면 일차적인 데이타 보호는 이루어진다. 그러나 키(key)의 완전한 비밀 유지가 어려우므로 수시로 키를 바꾸어야 한다.
이 방법의 또 다른 문제점은 키(key)의 추리가 가능한 점이다. 암호 해독 전문가가 다량의 메시지를 놓고 키를 추리해가면 어느 경우는 정확히 찾아낼 수가 있다.

가변 키에 의한 암호화 방법

단일 키에 의한 암호화 방법의 약점을 보완하여 연구된 방법의 가변 키에 의한 암호화 방법이다. 군사시설 또는 외교 채널간의 데이타 통신에서 키(key)가 노출되어 정보가 유출되는 것은 매우 불행한 일이다. 컴퓨터 네트워크 시스템에서 단일 키에 의한 데이타 암호화 방법은 믿을만한 것이 되지 못하게 되었고, 이것을 개선하여 연구한 결과가 가변 키에 의한 암호화 기법이다. 소위 이것을 안전한 키 교환을 위한 "프로토콜(protocols)"라고 부른다.

그림2 는 이 방법의 중심이 되는 개념을 보여주고 있다.

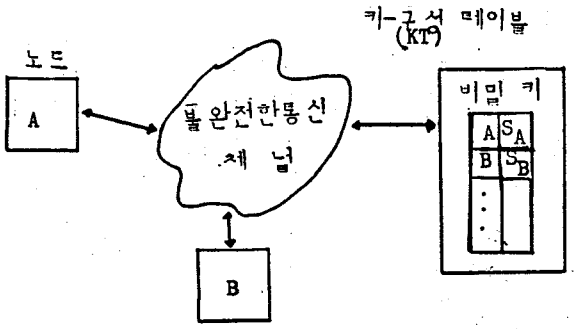

그림2. 가변 키에 의한 암호화

전송자 와 수신자 는 키-구성 테이블(KT) 로부터 비밀 키를 찾는다. 컴퓨터KT 는 비밀키에 대한 특수하게 고안된 리스트를 가지고 있어서 그중의 하나가 A, B 에 제공된다. 먼저A 와KT 사이에 비밀키 S_A 에 의거하여 암호화된 메시지 교신이 있게 된다. B 에게 송신할 결정을 내린뒤A 는KT 에게$(A,(I,B)^{S_A})$ 의 형으로 구성된 메시지를 보낸다. 여기서 I 는 A 에 의하여 임의로 선택된 메시지 구별자이다. KT 는 S_A 와I 에 의하여 결정되는

키인K를 생성한다. 그리고 A 에게 $(I,K,(K,A)^{S_B})^{S_A}$ 로된 메시지를 되보낸다. 단지, A 만이 이 메시지를 해독할 수 있으며, 이 메시지에 의하여 주어진 를 가지고 사이퍼텍스트(ciphertext)를 만드는 데 그 형식은 $(K,A)^{S_B}$ 로 구성된다. 그리고 이 사이퍼텍스트를 B 에게 전송한다. 이때 관계되는 비밀키의 요소는 S_A, S_B, I 그리고 K 이므로 이 메시지를 해독할 수 있는 자는 A 와 B 뿐이다. 그리고 I는 항상 바뀔 수 있으며 S_A 와 S_B 도 가변적으므로 그들에 의하여 생성되는 K는 당연히 가변적이다. 당사자인 A 와 B 는 SA 와 S_B에 대한 비밀 보완만 취하면 된다. 이 방법의 문제점은 절차가 복잡하고, 여러 노드간에 데이타 통신이 수행될 때 번거로움을 피하지 못하는 단점이 있는 점이다.

공중 키(public key)를 이용한 암호화

1976년에 Diffie 와 Hellman 에 의하여 처음으로 공중 키(public key)에 의한 암호화 개념이 연구 발표되었다. (DIFF 76a).

이 개념에서 하나의 사용자는 공중 키(public key)와 개인 비밀키로 된 두개의 키를 사용하게 된다. 공중 키는 교신하고자하는 상대방에게 공표해주나 개인 비밀키는 절대적으로 비밀유지를 해야 한다. 이 개념은 매우 좋지만 두 개의 키를 조합하여 암호화하는 알고리즘이 미약하면 역시 성능의 효율이 떨어지게 된다. 공중 키(public key) 의 기능과 공중 키의 제어에 대하여 기술하기로 한다.

공중 키(public key)의 기능

Diffie 와 Hellman 의 공중 키(public key) 모형에 의하여 공중 키의 기능을 기술하여 보기로 한다. 그림3은 공중 키를 이용하여 A에서 B로 메시지를 송신하는 과정을 보여준다. (DIFF 76b)

사용자는 공중 키(public key)분산 알고리즘에 의하여 공중 키를 생성한다. 단순하게 지수 함수로서 공중키(public key)를 작성할 수 있다. 즉, $Y = a^X$ 에 의하여 공중 키(public key) Y를 구성하는 데 a가 주어지면 자신의 비밀키 x를 대입하여 결과를 쉽게 얻게 된다. A에서 B로 송신할 때와 B에서 A 로 송신할 때의 경우와 또는 상대방의 비밀키를 알지 못하고 공중 키(Public Key)와 자신의 비밀키로 데이타를 암호화 및 해독하는 과정을 보자.

$Fx(a) = a^x$ 이고 $Fy(a) = a^y$ 라고 가정했으므로 $Fx\ Fy(a) = Fy\ Fx(a)$, 즉, $(a^y)^x = (a^x)^y$ 가 된다.

그림에서 $(2^4)^5 = 16^5 = 1{,}048{,}576$

$(2^5)^4 = 32^4 = 1{,}048{,}576$이 된다.

결론적으로, A 는 자신의 비밀키인 X_A를, B 는 X_B를 정하여 비밀을 보안하여 간직한다. 모든 X_i 는 공중 키(Public Key)를 계산할 때 사용된다. 변환 함수에 사용되는 a를 정하여 모든 사용자들이 알도록 공표한다. 따라서, 사용자A 는 $Y_B^{X_A}$ 를 계산하고 B 는 $Y_B^{X_B}$ 를 계산하게 되며 그 결과는 같아지게 된다.

여기에 사용되는 알고리즘에 따라 공중 키 (Public Key)의 성능은 크게 차이가 난다. RSA 기법에서는 mod 를 이용한 매우 강력한 알고리즘을 사용하고 있다 (Rive 78).

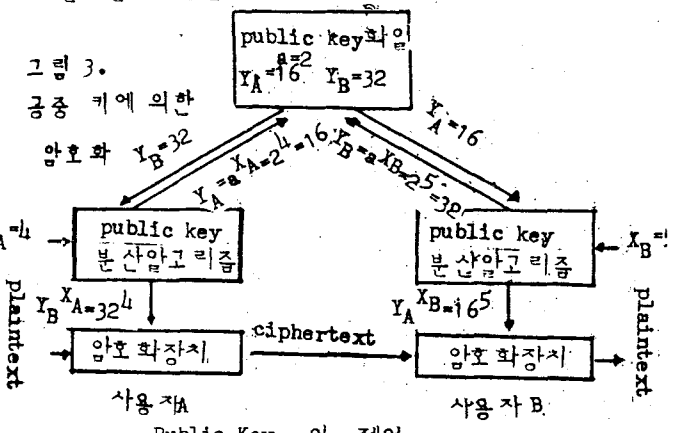

그림 3. 공중 키에 의한 암호화

Public Key 의 제어

Public Key 를 이용한 암호화가 아무리 완벽하게 이루어진다고 하더라도 Key 자체에 대한 교신이 잘못되어 오류를 범하는 경우는 문제가 된다. 컴퓨터 네트워크 시스템에서 Key를 어떻게 분산하여 제어할 것인가는 매우 중요하다. Host 컴퓨터를 두어 완전히 Key 제어권을 전담하게 할것인가, 또는 제어

권을 여러 노드에 분산할 것인가는 중요한 차이가 있다.

Public Key 제어 algorithm

중앙 집중 제어의 경우나 분산 제어의 경우에 문제시 되는 것은 시간이다.

또 하나가 키 제어 센터(KCC)에 들어 있는 키의 신뢰도이다. 왜냐하면 자신의 Key는 수시로 변경할 수 있기 때문에 어느 순간에는 키매칭이 실패할 수도 있다.

이 문제점을 함께 해결하는 방법을 기술하여 보자. 중앙 집중 시스템에서의 키 제어 센터나 또는 분산 시스템에서의 Key directory와 같은 유사한 기능을 갖는 authority를 규정하여 Key 확인 기능을 부여하기로 한다.

노드A 와 노드 B가 교신하고자 한다.

(1) A는 authority 에 시간표가 붙은 메시지를 보낸다.

(2) Authority는 A 에게 B의 Public Key(P_B)를 보낸다. 이때, A의 초기 메시지와 authority 의 Key 그리고 시간표를 함께 보낸다.

(3) 시간표에 의해 A는 authority 의 해독된 메시지를 확인한다. 그리고 자신이 보낸 초기 메시지를 확인한다.

(4) P_B 에 의하여 암호화한 메시지를 A는 B 에게 보낸다.

(5) B는 앞의 (1), (2) 단계와 같은 방법으로 authority 와 교신한다. 그리고 A의 Public Key (P_A) 를 얻는다. 또한 P_A 에 의해 암호화된 identifier 를 A 에게 보낸다

(6) A가 확인함으로서 A, B 간에 교신이 이루어진다. 그림4는 이 알고리즘을 도시한 것이다.

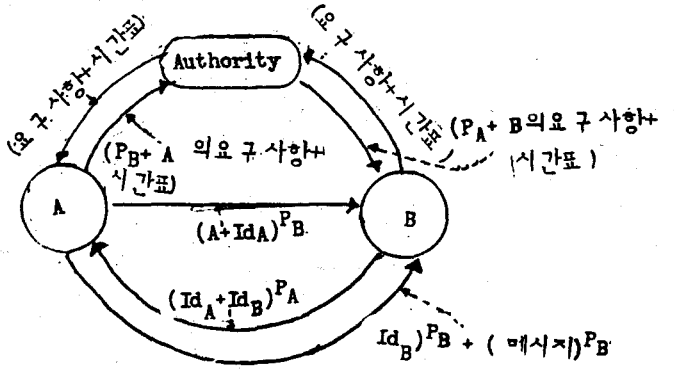

그림4. Public Key 제어 algorithm

Reference

(DENN 83) Denning,D.E,"Protecting Public Key and Signature Keys", Computer, IEEE,Feb. 1983

(DIFF 76a) Diffie,w, and M. Hellman,"Multiuser Cryptographic Techniques", Proceeding, 1976

(DIFF 76b) Diffie, W. and M. Hellman,"New Directions in Cryptography", IEEE, Trans. Inf. Theory IF22,Nov. 1976

(NEED 78) Needham,R.M. and M.D.Schroeder," Using Encryption for Authentification in Large Networks on Computers" CACM21, Dec. 1978

(POPE 78) Popek,G.J. and C.S. Kline,"Design Issue for Secure Computer Networks" ,Springer-Verlarg, New york,1978

(POPE 79) Popek,G.J. and et al,"Encryption and Secure Computer Networks", Computing Survey Vol. 11,Dec. 1979

(RIVE 78) Rivest,R.L. and et al,"A Method for Obtaining Digital Signature and Public Key Cryptosystems",CACM 21 Feb. 1978

(SIMM 79) Simmons,G.J.,"The Asymmetric Encryption/ Decryption Channel",Computing Survey 11, Dec. 1979