컴퓨터 통신망을 위한 암호화 프로토콜의 고찰 및 개선방안

허용도* · 손진곤** · 황종선*

* 고려대학교 전산과학과

** 한국방송통신대학 전자계산학과

< 요 약 >

정보화 사회가 전개되면서 대규모 컴퓨터 네트워크를 통해 정보나 자원을 서로 효율적으로 공유하는 것이 가능해졌고 이러한 정보나 자원의 공유현상으로 인하여 개인의 권리침해와 보안문제가 크게 대두되었다. 따라서 컴퓨터 통신에서는 이러한 정보나 자원을 효율적으로 관리할 수 있는 암호화 정책 및 메커니즘이 필요하다.

본 논문에서는 현재의 암호화 시스템에서 사용하는 암호화 방식과 사용자를 인증하기 위하여 사용되는 암호화 프로토콜을 비교분석하여 새로운 암호화 프로토콜을 제안하였다.

1. 서 론

컴퓨터 통신망은 하나의 거대한 컴퓨터 즉,하드웨어와 소프트웨어등의 자원등이 지리적으로 널리 분포되어 있는 단일 컴퓨터라고 생각 할 수가 있다. 이러한 거대한 컴퓨터의 가장 중요한 구성요소는 각각의 컴퓨터를 서로 연결시켜주는 통신 네트워크이다.[7] 따라서 사용자들이 통신 네트워크를 통해 정보나 자원을 서로 공유하는 것이 가능해졌고 정보나 자원의 공유현상으로 인한 보안문제가 크게 대두되었다. 컴퓨터 통신 네트워크를 통해 발생하는 많은 보안문제중 인증된 정당한 사용자만이 정보나 자원을 이용할 수 있도록 해주는 문제와 정보나 자원에 대한 허가를 받았다 하더라도 허용되지 않는 수정 및 불법 조작을 고의적으로 행하는 것으로 부터 정보나 자원을 보호하는 문제는 매우 중요하다. 그러므로 올바른 사용자를 인증하는 문제와 인증된 사용자가 안전한 통신을 통해 정보를 교환할 수 있도록 해주는 암호화 프로토콜이 필요하다.

본 논문은 2장에서는 컴퓨터 통신망에서 사용하는 암호화 방식을 공

통키 암호방식과 공개키 암호방식의 두가지로 나누어 살펴보았으며 3장과 4장에서는 기존의 암호화 프로토콜을 비교분석하여 새로운 암호화 프로토콜을 제안하였다.

2. 암호화 방식

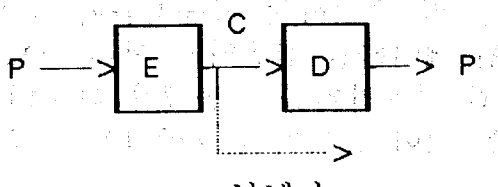
2.1 암호계의 기본 개념

정보나 자원의 보호란 컴퓨터 통신에 있어서 각종 정보나 자원을 침해자로부터 보호하는 것으로 그 목적은 정보나 정보의 불법적 노출을 방지하여 합법적인 사용자에게만 정보나 자원을 전달해주는 프라이버시(Privacy)와 정보나 자원의 불법적인 조작을 방지함으로써 송신자의 합법성을 보장시켜주는 인증(Authentication)에 있다. 따라서 암호학은 이러한 프라이버시와 인증의 두가지 문제를 해결하기 위한 수학적인 시스템에 관한 연구분야이며 암호계는 수학적 암호기법을 적용한 암호화 및 복호화 과정으로 구성된 시스템을 말한다.[9]

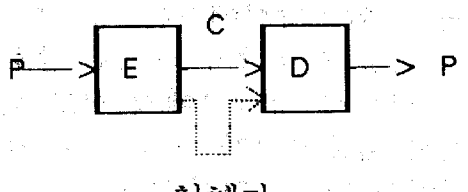
먼저 <그림 1> 은 프라이버시를 보호하기 위한 암호계의 기본 구성을 나타낸다.[6] 프라이버시 암호계에서 송신자는 평문 P를 암호화 알고리즘 E와 암호화키 K를 이용하여 암호문 C를 생성하며, 인정되지 않는 침해자가 감시하고 있는 통신채널을 통해 수신자에게 보내게 된다. 그러면 수신자는 이 암호문 C를 받아 복호화 알고리즘 D와 복호화키 K로 송신자가 보내고자 하였던 평문 P를 얻게 된다.

만일 이 때 침해자가 통신채널을 도청하여 암호문을 가로채게 되더라도 침해자가 복호화 알고리즘 및 복호화키를 알지 못한다면 암호문으로부터 평문을 얻을 수 없게 되어 데이타에 대한 프라이버시를 보증할 수 있게 된다.

또 <그림 2>는 송신자의 합법성을 보장해주는 인증암호계를 나타낸다.[6] 인증암호계에서 침해자는 통신채널을 통해 전송되는 데이타에 대해 단순한 감시뿐만 아니라 데이타의 추가, 삭제 및 조작을 할 수 있는 경우로서 이 경우에 대해서도 침해자가 불법적인 복호화 알고리즘과 복호화키를 가지고 통신채널에 전송되는 암호문을 조작하게 된다면 수신자는 암호문을 복호화시에 이것이 인증된 송신자에게서 온 정보인지를 확인할 수 있게 된다. 따라서 송신자에 대한 인증문제를 해결할 수가 있게 된다.



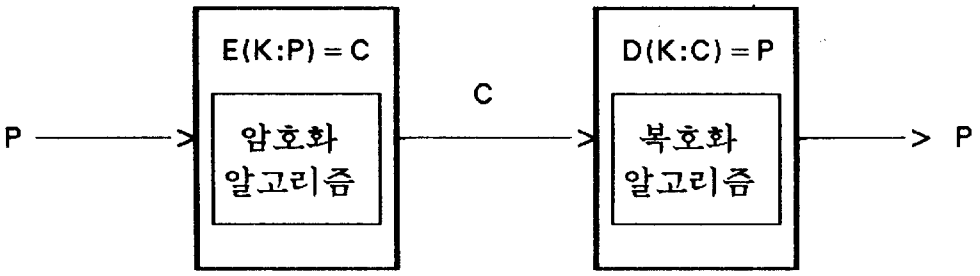
< 그림 1 > 프라이버시 암호계



< 그림 2 > 인증 암호계

2.2 공통키 암호방식

공통키 암호방식은 흔히 관용암호방식으로 불리우며 <그림 3>과 같이 정보를 교환하고자 하는 사용자들끼리 먼저 공통키 K를 침해자에게 노출되지 않게 나누어 갖은 다음, 보내고자 하는 평문 P를 공통키 K로 암호화한 암호문을 생성시켜 통신채널을 통해 전송하면 수신자는 공통키 K를 이용하여 암호문으로부터 평문을 얻는 방법을 말한다.[10]



< 그림 3 > 공통키 암호 방식

<그림 3>에서 E 와 D 는 각각 암호화, 복호화 알고리즘을 말하며 일반적으로 다음 세가지 조건을 만족하며 입력 (K:M) 에 대한 암호화 알고리즘 E의 출력을 E(K:M)이라 표시한다.

1) D(K:E(K:P)) = P는 임의의 키 K, 평문 P 에 대하여도 성립해야 한다.
2) E 와 D 의 효율이 좋아야 한다. 즉 어떠한 입력에 대해서도 출력을 계산하는 계산량이 적어야 한다.
3) 키 K를 1),2)의 성질을 갖는 임의의 알고리즘 (E,D)와 주어진 부대정보(Side Information)로부터 계산하는 계산량이 충분히 커야 한다.

이러한 공통키 암호화 방식에서 사용되는 암호화 알고리즘에는 환자(Substitution)식, 전치(Transposition)식, 혼합변환식(Product Cipher)등이 있으며 현재 가장 많이 사용되는 암호화 알고리즘 방식은 혼합변환식을 이용한 DES(Data Encryption Standard) 알고리즘이다.

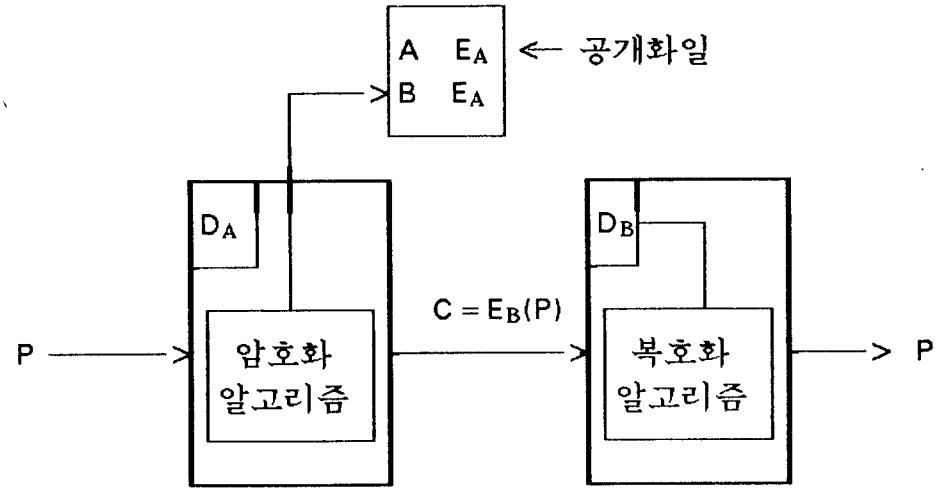
2.3 공개키 암호방식

공통키 암호방식에서는 정보를 송신 및 수신하는 사용자들이 동일한 하나의 키를 사용해야 하므로 암호화된 데이타를 전송하기 전에 어느 한쪽에서 반드시 상대방에게 서로 약속된 암호화키를 전송해야 하는데 이 과정에서 암호화키가 노출될 수 있다는 것이 공통키 암호방식의 가장 큰 문제점이라 할 수 있다.[10]

이를 해결하기 위한 새로운 암호방식으로 공개키 암호방식이 대두되었는데 이는 수학적 정수론에 근거를 둔 것으로 어떤 큰 수에 대한 소인수 분해과정이 시간적으로 불가능하다는 것을 이용한 것이다.[1] 즉 암호화에 사용하는 키와 복호화에 사용하는 키가 서로 다르기 때문에 침해자가 암호화키를 알아내도 암호화키로부터 복호화 키를 만들어 낼 수가 없는 것을 말한다. 따라서 공개키 방식에서의 사용자는 자신의 암호화키는 공개화일을 통하여 공개하고 복호화키만을 관리함으로써 공통키 암호방식에서 발생하는 키의 전송문제를 해결한다.

<그림 4>에서 보는 바와 같이 사용자 A가 사용자 B에게 정보를 전송할 경우 사용자 A는 먼저 공개화일을 검색하여 사용자 B의 공개키 E_B를 알아내고 이를 이용하여 보내려는 평문 P를 암호화 ($E_B(P)$)하여 사용자 B에게 전송하면 사용자 B는 자신만이 알고 있는 복호화키 D_B를 이용하여 암호문을 복호화 ($D_B(E_B(P))=P$)할 수 있다. 역으로 사용자 B가 사용자 A에게 정보를 전송할 경우에도 마찬가지 방법으로하면 된다.

이러한 공개키 암호방식에서 사용되고 있는 암호화 알고리즘에는 지수이론, Knapsack이론 등이 있으며 현재 가장 많이 사용되고 있는 알고리즘은 지수이론을 이용한 RSA 알고리즘이다.



<그림 4> 공개키 암호 방식

3. 기존의 암호화 프로토콜의 분석

3.1 Needham과 Schroeder의 프로토콜

Needham 과 Schroder에 의하면 컴퓨터 통신 네트워크의 각 사용자는 자신과 AS(Authentication Server)만이 사용자 자신의 암호화키를 알고있으며 상대방을 인증하기 위해 AS로부터 사용하는 양방향 규약(2-Way Handshaking) 함수를 침해자는 모른다는 가정하에 프로토콜을 제시하였다.[3]

즉, 사용자 A와 사용자 B가 AS를 사용할 경우 서로 통신을 하기 위해서는 AS로 부터 통신키를 다음 절차에 의해 분배를 받는다.

제 1 단계로 사용자 A는 사용자 B와 통신을 하기 위해 AS에게 자신의 식별자(I_A)를 보낸다. 제 2 단계로 AS는 사용자 A의 메세지로 부터 사용자 A를 인증하고 보안등급을 조사하여 사용자 B와 통신이 가능한지를 판별하고 통신을 허락할 경우 사용자 A의 공개키를 이용하여 메세지를 사용자 A에게 보낸다.

$$A \longrightarrow AS : A, B, I_A \qquad (1)$$

$$AS \longrightarrow A : K_A(I_A, B, CK, Y) \qquad (2)$$

$$Y = K_B(CK, A)$$

제 2 단계가 끝나면 사용자 A는 응답 (2)가 이전의 응답의 재전송이 아닌것을 알 수 있다. 제 3 단계에서 사용자 A는 사용자 B에게 AS로부터 받은 정보 Y를 전송해준다.

$$A \longrightarrow B : Y \qquad (3)$$

제 4 단계에서 사용자 B 는 자신의 복호화키를 이용하여 사용자 A로 부터 온 정보 Y를 복호화하여 통신키 CK를 얻을 수 있고 이것이 사용자 A로 부터 온 정당한 통신인지 혹은 침해자로부터의 재전송인지를 파악하기 위하여 새로운 식별자 (I_B)를 통신키 CK로 암호화하여 사용자 A에게 전송한다. 제 5 단계에서 사용자 A는 사용자 B에게 통신키가 자기로부터 전달되었음을 알려주는 식별자의 변환값을 사용자 B에게 재전송한다.

$$B \longrightarrow A : CK(I_B) \qquad (4)$$

$$A \longrightarrow B : CK(f(I_B)) \qquad (5)$$

3.2 Denning 과 Sacco 의 프로토콜

Needham과 Schroeder의 재전송 문제점을 해결하기 위하여 Denning과 Sacco 는 "Time Stamp" 라는 방법을 프로토콜에 적용하였으며 각 사용자의 암호화키가 누설되지 않았다는 가정하에 양방향 규약(2-Way Handshaking)함수를 사용하지 않아도 되는 키분배 프로토콜을 제시하였다.[2]

Denning 과 Sacco 의 프로토콜은 아래와 같다.

사용자 A 와 사용자 B가 서로 통신을 할 경우 AS 로 부터 통신키를 분배 받기 위해 다음 과정을 거친다.

$$A \longrightarrow AS : A, B \qquad (1)$$

$$AS \longrightarrow A : K_A(B, CK, T, Y) \qquad (2)$$

$$A \longrightarrow B : Y \qquad (3)$$

$$Y = K_B(CK, A, T)$$

여기서 Time Stamp T 는 침해자에 의한 재전송을 막기 위한 것으로 다음 조건을 검사한다.

$$| CLOCK - T | < \triangle t1 + \triangle t2$$

여기서 CLOCK 은 각 호스트에서 제공하는 지역시간을 의미하고 △t1 은 AS의 시간과 각 사용자와의 시간차를 나타내고, △t2 는 예상되는 네트워크 지연시간이다. 따라서 각 노드에서 처음에 기준치 시계를 참조한다면 T에 의해 제 3자에 의한 재전송 문제를 해결할 수 있다. 왜냐하면 K_A와 K_B가 누설되지 않는다면 AS만이 T를 암호화 할 수 있으며 사용자 A와 사용자 B는 안전하게 통신키 CK를 사용할 수가 있을 것이다.

3.3 암호화 프로토콜의 비교분석

Needham 과 Schroeder 의 프로토콜은 AS가 양방향 규약(2-way Handshaking)함수와 통신키 및 암호화키를 분배하는 것으로 AS는 모든 것을 알고 있으며 AS로 부터 분배되는 암호화키는 AS가 가지고 있는 암호화키로 암호화되어 전송되므로 제 3자도 AS의 암호화키를 이용하여 상대방의 암호화키를 쉽게 획득할 수 있다. 특히 각 노드의 암호화키와 양방향 규약(2-way Handshaking)함수는 각 노드에서 직접 관리해야 하며 이들이 노출될 경우 침해자로부터의 재전송이 가능해진다.

또한 Denning과 Sacco의 프로토콜은 Time Stamp라는 개념을 적용하여 재전송 문제를 해결한 것이나 AS의 암호화키를 이용하여 통신키를 분배받기 때문에 침해자는 쉽게 암호화키를 획득할 수 있으며 획득한 암호화키로 어떠한 정보도 암호화하여 전송할 수 있어 정보의 진위 판별이 곤란하다. 이 두가지 프로토콜을 비교하면 <그림 5>와 같다.

protocol	Needham 과 Schroeder	Denning 과 Sacco
특징	2 way Handshaking 함수 이용	Time Stamp
통신대상	노 출	노 출
통신키	AS나 제 3자에게 노출	AS나 제3자에게 노출
암호화키	AS 에게 노출	AS 에게 노출
키생성및 분배	AS에서 생성,분배	AS에서 생성,분배
키분배	RSA Alg.	RSA Alg.
자료전송	DES Alg.	DES Alg.
단점	재전송이 가능	통신키 노출

< 그림 5 > 각 프로토콜의 비교

4. 개선된 암호화 프로토콜 방식

4.1 기존의 암호화 프로토콜의 문제점

3 장에서 살펴본 두개의 암호화 프로토콜은 각각 사용상의 많은 문제점들을 노출시킬 수 있다.

먼저 Needham과 Schroeder의 프로토콜은 양방향 규약 함수와 사용자 A의 암호화키가 누설되지 않았다는 가정하에 프로토콜을 정의하였다. 따라서 양방향 규약 함수를 AS로 부터 분배받아 각 사용자 노드에서 관리해야 하며 AS의 암호화키는 제 3자에게도 쉽게 노출될 수 있으므로 누구나가 AS의 통신키를 쉽게 해독할 수 있다. 또한 사용자 A의 암호화키가 노출될 경우 침해자에 의한 정보의 재전송이 가능하다라는 것도 큰 문제점이라 할 수 있다.

또한 Denning과 Sacco의 프로토콜은 Time Stamp 라는 개념을 도입하여 침해자에 의한 정보의 재전송을 방지하였으나 AS의 암호화키를 이용하여 통신키를 분배하기 때문에 침해자가 쉽게 암호화키를 획득한다면 획득한 암호화키로 통신키를 쉽게 얻어낼 수가 있다. 그러므로 암호화하여 전달된 정보의 인증이 어렵다.

따라서 기존의 암호화 프로토콜에서 발생하는 문제점을 해결하기 위하여 개선된 암호화 프로토콜을 4.2 절에 제시하였다.

4.2 개선된 암호화 프로토콜

개선된 암호화 프로토콜은 기존의 암호화 프로토콜과 비교하여 가장 큰 차이점은 통신하려는 사용자가 서로를 인증하는데 있어서 AS의 암호화키를 사용한다는 것을 들 수 있고 각 사용자의 식별자로는 난수를 이용하게 된다. 또한 정보를 송신 및 수신하는데 있어서 사용되는 암호화키와 복호화키는 기존의 RSA알고리즘을 이용하여 생성한다는 것을 들 수 있다. 따라서 AS의 역할은 통신하려는 사용자의 보안등급을 결정하여 통신을 허락한다는 메세지를 상대방에게 전달할 뿐만 아니라 통신대상이 올바른지를 판단하는 인증기능을 갖게된다.

즉 사용자 A가 사용자 B와 통신하기 위해서는 먼저 AS에게 사용자 B와의 통신이 가능한지를 확인한다.

$$A \longrightarrow AS : A,B \qquad (1)$$

이 때 AS는 보안등급을 조사하여 통신이 가능한지를 검사하고 통신이 가능하다면 사용자 A 를 인증하기 위하여 임의의 식별자 I_{AS} 를 사용자 A에게 송신한다. 따라서 사용자 A가 AS로 부터 통신을 해도 좋다는 허락을 받으면 사용자 A는 사용자 B에게 AS로 부터 받은 모든 정보와 자신의 암호화키를 E_{AS}를 이용하여 암호화 하여 송신한다.

$$AS \longrightarrow A : E_{AS}, E_{AS}(I_{AS}) \qquad (2)$$

$$A \longrightarrow B : E_{AS}, E_{AS}(I_{AS}), E_{AS}(E_A, I_A) \qquad (3)$$

다음으로 사용자 B는 사용자 A에게 해독할 수 없는 정보를 받게되면 그것이 누구한테 온것인지를 확인하기 위하여 수신한 모든 정보를 AS에게 모두 전송한다.

B —> AS : $E_B, E_{AS}, E_{AS}(E_A, I_{AS}, I_A, I_B)$ (4)

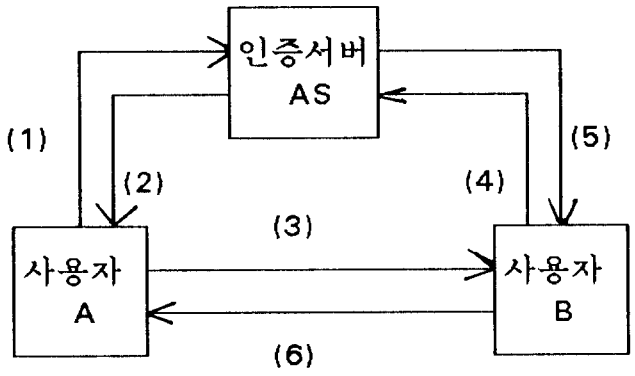
AS는 사용자 B로부터 송신된 정보를 자신의 복호화키를 이용하여 해독하여 사용자 A의 식별자 및 암호화키를 사용자 B에게 보낸다. 이 때 식별자 및 암호화키는 사용자 B의 암호화키를 이용하여 송신된다.

AS—> B : $E_B(E_A, I_A, I_B)$ (5)

그러면 사용자 B 는 사용자 A의 식별자 및 암호화키를 이용하여 통신하려고 하는 사용자가 누구인지를 알게되고 사용자 A의 식별자를 다시 돌려준다.

B —> A : $E_A(I_A)$ (6)

위와 같은 암호화 프로토콜을 도해로 나타내면 <그림 6>과 같다.



< 그림 6 > 개선된 암호화 프로토콜

5. 결 론

본 연구에서는 암호화 프로토콜의 문제점을 해결하기 위한 한 방편으로 통신키의 분배과정에 대해서 살펴보고 개선된 암호화 프로토콜을 제안하였다.

4.2절에서 제안한 암호화 프로토콜은 기존의 암호화 프로토콜과 비교해 볼 때 통신키를 매번 반복해서 생성해내지 않고, AS가 가지고 있는 암호화키를 이용해서 모든 식별자를 송신하기 때문에 통신하려는 상대방을 정확하게 인증할 수 있다는 장점이 있다. 그러나 사용자 B가 사용자 A로 부터 정보를 받으면 그 정보를 해독하기 위하여 AS에게 모든 정보를 송신하고 AS로 부터 해독된 정보를 받아야하기 때문에 컴퓨터 통신망을 이용하는 사용자가 많은 경우에는 통신오버헤드가 커진다는 것을 단점으로 들 수 있다. 따라서 본논문에 이어 연구되어야 할 분야는 이러한 통신오버헤드를 줄이는 방법과 AS에서 각 사용자의 보안등급을 결정할수 있도록 해주는 보안 정책 및 메커니즘에 관한 연구등이 수행되어야 할 것이다.

<참고문헌>

[1] Gerald J.Popek and Charles S.Kline,"Encryption and Secure Computer Networks",ACM Computing Surveys,Vol.11,No.4,Dec.1979

[2] Dorothy E.Denning and Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols", Comm. ACM, Vol.24,NO.8, Aug.1981

[3] Needham.R. and Schroeder.M, "Using encryption for Authentication large networks of computers", Comm. ACM, Vol.21,NO.12, Dec. 1978

[4] Carl E.Landwehr, "Formal Models for Computer Security", ACM Computing Surveys, Vol.13,NO.3, SEP.1981

[5] David B.Newman, Jr.Jim K.Omura Raymond L.Pickholtz, "Public Key Management for Network Security", IEEE Network Magazine, Vol.1,NO.2,Apr.1987

[6] W.Diffie and M.E.Hellman, "Privacy and Authentication: An Introduction to Cryptography", Proc. IEEE, Vol.67,No.3, Mar.1979.

[7] Jennifer Seberry and Josef Pieprzyk, "Cryptography:An Introduction to Computer security", Prentice Hall, 1989.

[8] 남길현, "암호시스템의 특성과 활용",한국정보과학회지 제 7권 제 5호, 1989.10.

[9] 정진욱, "암호학 이론", 한국 정보과학회지 제 7권 제 5호, 1989.10.

[10] 이종완, "분산 컴퓨터 시스템에서 키분배 프로토콜에 관한 연구",고려대학교, 석사학위논문, 1990.11.