타원곡선 암호체계 및 IPSEC을 이용한 안전한 메신저 설계

박수영° 최광미 정채영
조선대학교 전산통계학과
e-mail:{swiminpark, iplab}@hanmail.net
cyjung@chosun.ac.kr

Design On a Secure Messenger Using Elliptic Curve Cryptography and IPSec

Su-Young Park° Gwang-mi Choi Chai-Yeoung Jung
Dept. Computer & Statistics. Chosun University

요 약

현재 사용되고 있는 대부분의 메신저는 서버에 로그 온할 때 패스워드를 RC5등으로 암호화해서 보내지만 패스워드 크래킹 프로그램들이 많이 알려져 있어 안전하지 못하다. 또한 로그 온한 후 통신하는 두 호스트들 간의 전송되는 정보가 아무런 보호 장치 없이 네트워크를 통해 전송되어 제3자에 의한 도청이 가능하게 된다. 따라서 전송되는 정보의 암호화를 포함하는 안전한 메신저 서비스의 필요성이 대두되고 있다. 본 논문에서 제안된 안전한 메신저는 동일한 키 사이즈를 갖는 다른 공개키 암호체계보다 훨씬 강하다고 알려져 있는 타원곡선 암호체계를 이용하여 빠르고 효율적이며 높은 안전도를 나타내는 패스워드 키 교환 방식을 설계하였고, 사용자간에 IPSec프로토콜을 사용하여 효율적인 데이터 전송이 가능하고 또한 보안성을 높이기 위한 방법으로 Host-to-Host간의 데이터가 인터넷에서 가상의 파이프를 통해 전달되도록 터널 모드를 제시하였다.

1. 서 론

최근 인터넷을 기반으로 하는 정보통신 인프라의 발달에 따라 다양한 서비스가 등장하였고 그 응용분야 또한 광범위하다. 특히, 전자우편 서비스는 기존 우편 서비스를 대체할 수 있을 정도로 강력한 기능 및 편리성과 신속성으로 대중화에 성공하여 많은 사용자들을 확보한 실정이다. 이러한 상황에서, 몇 년 전부터 제공되기 시작한 메신저는 전자우편, 파일전송 및 채팅 등의 기존 서비스를 통합하고 부가적으로 다양한 최신 서비스들까지 제공하는 새로운 형태의 서비스를 제공하고 있어 그 이용자가 계속 증가하고 있는 실정이다.

현재 사용되고 있는 대부분의 메신저는 전송되는 정보에 대한 보안 기능이 없는 상태로 운영되고 있다. 이렇게 메신저 서비스 사용자의 개인정보나 전송되는 메시지가 아무런 보호장치 없이 네트워크 상에 노출되어 있는 상황은 제3자에 의해 그 정보가 도청될 수 있는 잠재적 보안 위험을 내포하고 있다. 따라서 전송되는 정보를 안전하게 전달하는 안전한 메신저 시스템 개발이 필요하다. 이에 본문에서 제안한 안전한 메신저는 무선 인터넷 환경에서 안전하고 신뢰할 수 있는 ECC를 이용한 키 교환 방식과 공중 인터넷 망을 통해 전달되는 패킷의 보호를 위해 고안되어진 IPSec 프로토콜을 이용하여 통신하는 두 호스트간의 정보를 암호화하여 전송하도록 설계하였다.

2. 관련연구

2.1 개요

메신저의 발상은 단순하다. 메신저를 쉽게 정의한다면 사용자 A가 사용자 B에게 어떤 문자열을 전송하는 것이다. 즉, TCP/IP 프로토콜을 이용하여 인터넷이 연결된 곳이라면 언제 어디서나 실시간으로 메시지를 주고받을 수 있는 프로그램을 의미한다[1~6]. 메신저의 주요 기능은 텍스트 메시지를 신속하게 실시간으로 상대방에게 전달하는 것이지만 다양한 기능들을 포함한 새로운 메신저들이 등장하고 있는 실정이다.

메신저는 구현 형태에 따라 크게 표 1처럼 두 가지 형태로 구분 할 수 있다.

<표 1> 두 가지 형태의 메신저 비교

	서버 종속형	서버 독립형(P2P)
특 징	· 대규모 네트워크에 적합	· 소규모 네트워크에 적합
	· 중앙 서버에 존재	· 서버가 필요없음
	· 서버에 의한 작업 통제	· 다양한 프로토콜 이용가능
장 점	· 안정적 · 효과적인 메시지 작업 가능	· 소규모 단체 내부에서 신속하고 간단한 메시지 전송
	· 다양한 서비스 및 기능 제공	

	· 광고효과	
	· 지역적 제한 없음	
단 점	· 시스템 관리 및 유지보수 난이	· 다양한 서비스 제공의 한계
	· N/W 단절로 인한 전체 기능 이용 불가	· 지역적 제한
종 류	· 대부분의 메신저	· Win95/98의 WinPopup

2.2 보안 문제점

기존의 메신저 서비스들은 서버에 로그 온할 때 패스워드를 RC5등으로 암호화해서 보내지만 최근에 패스워드 크래킹 프로그램들이 많이 알려져 있는 상태이다[7]. 또한 클라이언트 메신저간의 전송되는 정보가 아무런 보호 장치 없이 네트워크를 통해 전송되므로 제3자가 이를 도청하거나 전송 메시지가 노출될 수 있으므로 개인정보 유출에 대한 보안 문제점들이 제기되고 있다.

따라서 본 논문에서는 무선 인터넷 환경에서 안전하고 신뢰할 수 있는 ECC를 이용한 패스워드 키 교환 방식과 IPSec을 이용하여 클라이언트 간의 전송되는 정보의 암호화 및 사용자 인증을 지원하여 안전하게 정보를 전달할 수 있도록 하는 안전한 메신저 메커니즘을 설계하였다.

3. ECC 및 IPSec

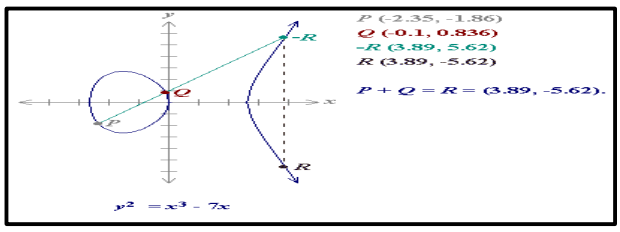
3.1 ECC의 개요

ECC는 특정 암호 알고리즘이 아닌 암호 알고리즘을 구현해 볼 수 있는 수학적인 장소를 제공하고 있는 것으로 기존의 정수 공간이 아닌 타원 쌍곡선위에서 구현을 한 것이다[8, 9].

유한체 $GF(p)$(p>3인 소수)상의 타원곡선은 다음과 같은 Weierstrass 방정식을 만족하는 $GF(p)$상의 모든 점 (x, y)와 가상의 무한원점(point at infinity) O로 구성된다. 실수 위에서 정의된 타원곡선이라 함은 식 3-1의 타원곡선 방정식을 만족시키는 점(x, y)들의 집합이다.

$$y^2 = x^3 + ax + b,\ (x, y, a, b\text{는 모두 실수})\ \text{(식 3-1)}$$

여기에서 계수들은 다음 조건, $4a^3 + 27b^2 \neq 0$을 만족시킨다면 이 타원곡선은 실제로 이 타원곡선 상에 존재하지 않는 무한 원점(point at infinity) O와 함께 하나의 군을 형성한다. 실수에서 정의된 타원곡선은 계산이 느리고 반올림에 의한 오차로 인하여 계산이 부정확하고 구현하는 원소 {0,1}을 사용하므로 암호에는 적당하지 않다. [그림 3]은 실수 타원곡선 상의 서로 다른 두 점의 덧셈의 예이다.



(그림 3) 실수 타원곡선 상의 다른 두 점의 덧셈의 예

$GF(2^m)$상에서 정의된 타원곡선 군은 유한개의 원소를 가지게 되고 반올림에 따른 오름차가 전혀 없기 때문에 이진 컴퓨터 연산에 많이 쓰이게 된다. P와 Q를 타원곡선 E위의 두 점이라 하면 아래 같은 연산 공식이 성립한다. 식 3-2는 유한체 $GF(2^m)$에서의 타원곡선 방정식이다.

$$y^2 + xy = x^3 + ax^2 + b,\ (a, b \in GF(2^m))\ \text{(식 3-2)}$$

[$GF(2^m)$상의 점 덧셈 연산 알고리즘]

◎ $P \neq Q$이면, $P+Q=R(x_3, y_3)$이고, x_3, y_3의 값은 다음과 같다.

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a,$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$
$$\lambda = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)$$

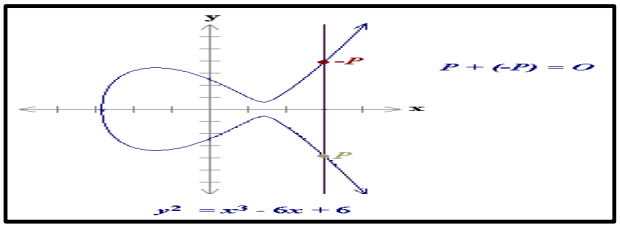
$Q = xP$을 구하는 덧셈 연산은 모듈러 곱셈을 통해 이루어진다. 주요 공개키 암호시스템은 효율적인 모듈러 곱셈에 의존하고 있으며, 타원곡선은 소수 P의 값이 서로 다른 시스템보다 작기 때문에 그 효율성이 뛰어나다 할 수 있다. 즉, 타원곡선 암호시스템의 안전도는 타원곡선 이산대수 문제에 의존하고 있으며, 그 효율성은 xP의 빠른 계산에 달려 있다. [그림 4]는 $GF(2^m)$상의 덧셈에 대한 역원과 무한 원점의 예이다.

3.2 IPSec의 개요

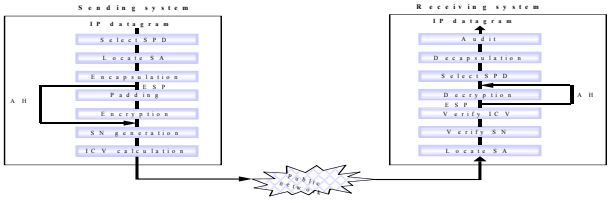
IPSec(Internet Procotol Security)은 IETF (Internet Engineering Task Force)에 의하여 표준화된 VPN 터널링 프로토콜로 IP의 확장된 형태이며 TCP/IP 기반의 네트워크 상에서 운용된다. 이것은 보호하는 데이터 영역에 따라 터널 모드와 트랜스포트 모드로 구분된다. 터널 모드(tunnel mode)는 보안 게이트웨이에서 다른 보안 게이트웨이로 안전하게 정보를 전송하기 위하여 새로운 IP 헤더를 덧붙여서 IP데이터그램 전체를 캡슐화 하고, 양쪽의 보안 게이트웨이들의 IP 주소를 새로운 IP 헤더의 주소 필드에 사용한다. 트랜스포트 모드(transport mode)는 호스트에서 호스트로 안전하게 정보를 전송할 수 있도록 IP 페이로드를 캡슐화 한다[12,13]. IPSec 보안 프로토콜로는 인증, 데이터의 무결성 및 리플레이 방지를 위한 AH(Authentication Header)프로토콜과 인증, 데이터의 무결성, 리플레이 방지와 기밀성을 위한ESP(Encapsulating Security Payload)프로토콜이 있다[10, 11].

이 두 가지 프로토콜은 각각의 요구수준에 따라 독립적으로 사용될 수도 있고, 조합된 형태로 사용될 수도 있다. AH는 HMAC-MD5나 HMAC-SHA와 같은 메시지 압축함수를 통하여 [그림 5]와 같이 IPSec에서 제공하는 각 모드에 따라 일정 영역을 압축하고, 그 값인 ICV(Integrity Check Value)를 AH 헤더 상의 인증 데이터(Authentication Data) 필드 값으로 사용한다. 이 값을 통하여 인증과 데이터의 무결성을 보장하고 일련 번호(Sequence Number : SN)의 생성과 일련 번호의 검증으로 리플레이 방지 기능을 제공한다[10,11,12].

ESP는 DES 혹은 RSA와 같은 메시지 암호화 함수로 각 모드에 따라 일정영역을 암호화하여 보냄으로써 데이터의 기밀성을 보장하며 AH와 동일하게 일련번호를 통하여 리플레이 방지 기능을 제공한다[13,14].



(그림 4) 덧셈에 대한 역원과 무한 원점

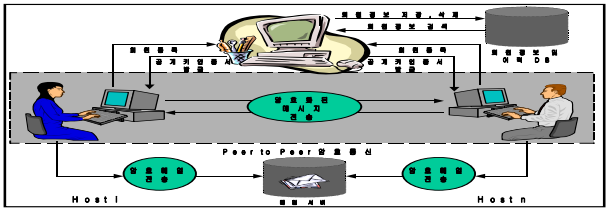


(그림 5) IPSec Procedure

4. 제안된 메신저 메카니즘

4.1 구조

본 논문에서 제안하는 메신저는 메신저 클라이언트, 메신저 서버, 회원정보 및 이력 DB, 메일 서버 등 이상의 네 가지 구성요소들로 이루어진다. 개략적인 시스템 구조도는 [그림 6]과 같다.



(그림 6) 메신저 구조

4.2.1 등록 및 접속

처음 사용자가 안전한 메신저를 실행하면 사용자가 안전한 메신저에 가입하거나 메신저에 접속하는 경우에 전송되는 개인 정보는 암호화되어 전송되어야 한다. 기존에는 패스워드를 대칭키 암호기술로 암호화해서 보내지만 패스워드 크래킹 툴이 많아 알려져 있어 안전하지 못하다. 따라서 본 논문에서는 동일한 키 사이즈를 갖는 다른 암호체계보다 훨씬 강하다고 알려져 있는 타원곡선 암호체계를 이용하여 패스워드 키 교환 방식을 제안한다. 등록절차를 거쳐 서버의 검증을 받은 클라이언트는 서버로부터 전송받은 공개키를 가지고 *ID, PWD*를 타원곡선 암호 알고리즘으로 암호화해서 보내지고 [그림 7]은 클라이언트가 서버에게 *ID, PWD*를 보내는 과정을 보여주고 있고, [그림 8]는 서버가 *ID, PWD*를 검증하는 과정을 보여주고 있다. 서버는 데이터베이스에 저장된 클라이언트의 개인키 인증서를 찾아서 복호화 한다.

타원곡선 E와 $P(\in E)$를 공개하고,
메시지 $M=(ID_x, PWD_y)(\in F_{2_m} x\ F_{2_m})$이라 가정하자.

< *Client*(메신저 사용자)가 *Server*에 로그인 할 때>

[Server]

임의로 정수 a를 선택

kP를 계산하여 공개

[Client]

임의로 정수 k를 선택

점 kP와 점 $k(aP)=a(kP)=(x, y)$를 계산

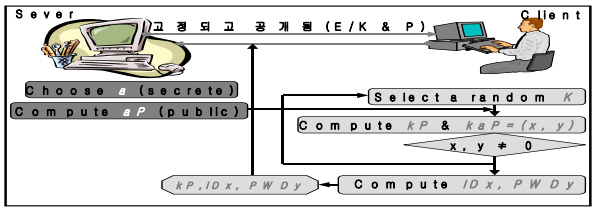
$x, y \neq 0$이면,

$(kP, IDx, PWDy)$를 *Server*에게 보낸다.

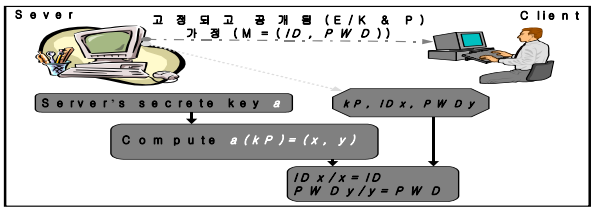
<*ID, PWD*를 확인하기 위하여(Server)>

1) $a(kP)=(x, y)$를 계산

2) $\frac{IDx}{x} = ID$, $\frac{PWDy}{y} = PWD$



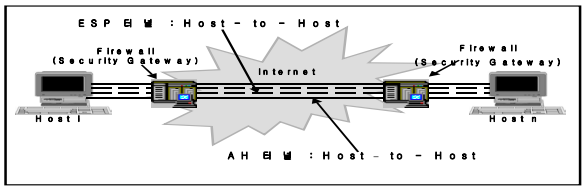
(그림 7) 클라이언트가 서버에게 *ID, PWD*를 보내는 과정



(그림 8) 서버가 *IP, PWD*를 검증하는 과정

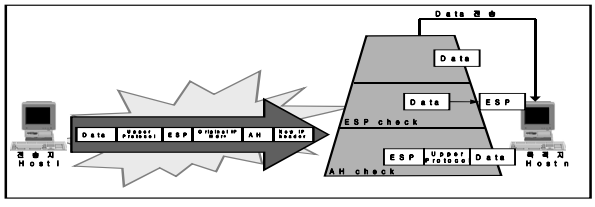
4.2.2 암호화된 대화 기능

암호화된 대화 기능은 온라인 상태에 있는 사용자간의 암호화된 호스트 간 채팅을 수행하는 기능으로써, 사용자 A가 B에게 채팅을 요청하여 상호간의 메시지 송수신 중에 암호화된 메시지를 전송하는 기능을 수행한다. 이때 제약사항으로는 채팅하는 사용자는 인증서가 배포된 등록된 그룹멤버이어야 하고 IPSec프로토콜을 사용해야 한다. [그림 9]은 IPSec프로토콜 환경의 터널링을 기반으로 하는 예이다.



(그림 9) 제안된 IPSec을 이용한 메시지 교환 메커니즘

두 호스트 간에 터널이 형성되면 호스트는 메시지를 ESP로 캡슐화 하여 전송한다. 비인증된 변형으로부터 데이터그램을보호하기 위해서는 AH를 반드시 사용해야 한다. AH와 ESP로 캡슐화된 메시지를 전송하는 동작원리는 [그림 10]와 같다.



(그림 10) 제안된 메시지 전송 메카니즘

5. 결론

IDC 보고서에 따르면 2003년 전 세계적으로 1억 3천명 정도가 무료 메신저를 사용하고 있으며 이중 8천만 명 정도는 매일 메신저를 이용하고 있는 것으로 나타났고 메신저의 사용은 앞으로 점점 늘어날 것으로 전망된다. 메신저가 보다 활성화되기 위해서는 안전성 및 신뢰성을 보장 할 수 있는 정보보호가 필요하다. 본 논문에서는 처리 속도가 빠르고 비트 당 안전도가 타 공개키 시스템 보다 효율적인 ECC와 네트워크 계층에서 직접적인 패킷 보안을 제공하는 IPSec에 대해 살펴보고 메신저에 적용할 수 있는 방법을 고찰 해 보았다.

본 논문은 타 암호시스템보다 처리속도가 빠르고 강한 ECC 암호 알고리즘을 사용하여 서버에 로그인 함으로써 개인의 프라이버시 침해 문제 등을 해결하고자 했다. 또한, IPSec 터널을 이용하여 데이터를 전송하게 함으로써 데이터에 대한 인증과 기밀성 서비스를 제공하도록 하였다. 향후 메신저가 현재보다 발전하기 위해서는 연구에만 전념하지 말고 연구를 통해 제안된 시스템을 실질적으로 구현하는 방향으로 연구가 진행되었으면 한다.

참 고 문 헌

[1] “빠른 세대의 빠른 통신법, 인스턴트 메시징”, 마이크로소프트웨어, pp.254-289,1999.
[2] RFC 2778("A Model for Presence and Instant Messaging"), http:// www.ietf.org/rfc/rfc2778.txt
[3] RFC 2779("Instant Messaging/Presence Protocol Requirements"), http:// www.ietf.org/rfc/rfc2779.txt
[4] "Common Presence and Instant Messaging Message Format",http://www.ietf.org/internet-drafts/draft-ietf-impp-cpim-msgfmt-03.txt.
[5] "Data and Time on the Internet: Timestamps", http://www.ieft.org/internet-drafts/draft-ietf-impp-datetime-04.txt.

[6] "CPIM Presence Information Data Format", http://www.ieft.org/internet-drafts/draft-ietf-impp-cpim-pidf-00.txt.
[7] “Instant Messaging 서비스의 기술동향 및 안전성 분석”, (주)퓨쳐시스템 정보통신연구소 암호체계센터, FS-TR01-09, Dec, 22, 2001 (20 pages).
[8] A.J Menezes and S. A. Vanstone, "Elliptic Curve Cryptosystems and her mplementation, Journal, on Crytology, PP 209-224, Autumn, 1993.
[9] ECC Toturial, http://www.certicom.com/resources/ecc_toturial/ecc_toturial.html, 2001.
[10] S. Kent. et. al., "Security architecture for the Internet Protocol," RFC 2401, IETF. 1998.11.
[11] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November 1998
[12] S. Kent, R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC 2406, November 1998.
[13] C. Madson, R. Glenn, "The Use of HMAC-MD5 within ESP and AH", RFC 2403, November 1998.
[14] C. Madson, R. Glenn, "The Use of HMAC-SHA-1 within ESP and AH", RFC 2404, November 1998.