인터넷상에서 타원 곡선 암호화 알고리즘을 이용한 가상 사설망의 설계

이주훈, 전문석, 이철희
숭실대학교 전자계산학과 대학원

Virtual Private Network design using Elliptic Curve Cryptography in Internet

Ju-Hun Lee, Moon-Seog Jun, Cheol-Hea Lee
Graduate School of Computing, Soongsil University

요 약

인터넷의 급성장은 전세계의 전반적인 사회 구조를 급변화시킨 원동력이 되었다. 하지만 사용자의 급증으로 인한 인터넷의 주소가 한계에 다달았다. 그래서 많은 기업이나 공공 기관에서는 각자의 사설망을 구축하여 사용하지만 지역적으로 멀리 떨어진 지점과의 통신상의 해킹 문제점들이나 전용선을 이용할 경우 상당한 비용의 문제점이 발생하였다. 본 논문에서는 기존 사설망을 이용하여 지역적으로 멀리 떨어진 지점과도 하나의 사설망으로 구축하여 인터넷을 사용할 수 있도록 하였다. 또한, 인터넷을 통하여 전송되는 데이터의 해킹 문제를 해결하기 위해 타원 곡선 알고리즘을 이용하여 보다 안전하게 전송할 수 있도록 하였다.

1. 서 론

수많은 네트워크가 인터넷에 연결되어 있어, 수 많은 정보들이 인터넷을 통해 전달되고 있다. 이 중에는 사적인 정보들이나 중요한 정보들이 전달되고 있지만, 이 정보들은 완전히 노출된 상태이기 때문에 해커들에 의해 중요한 정보들을 절취당한다. 특히 전자상거래가 활발해지면서, 신용카드 넘버나 비밀번호라든지 다른 중요한 정보들이 사용자도 모르는 사이에 사용되어 개인적으로 상당한 피해를 당하는 사례도 늘고 있다. 또는 중요한 공공기관이나 거대 기업에 침입하여 중요한 정보를 가져가거나 시스템을 사용할 수 없도록 망가뜨려 큰 피해를 가져오거나 이러한 행위를 사전에 방지하고자 많은 방법들이 제시되었지만 이것 역시도 완벽하게 방지할 수 있는 제안이나 시스템들은 개발되지는 못하였다.

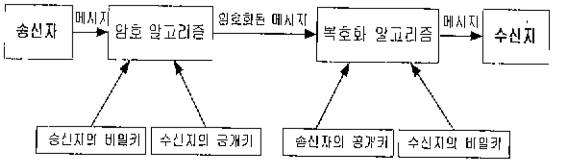
이를 위해 기업들은 인트라넷이라는 사설망을 구축하여 지사내에서 인터넷을 통하지 않고, 데이터를 공유하고 중요한 문서를 전달할 수 있게 되었다. 하지만 해외에 지사를 두거나 지역에 지사를 둔 거대 기업들은 전용선을 이용하여 사설망을 연결하기란 비용면에서 많은 부담을 주거나 또한 인터넷을 통하여 회사의 중요한 정보를 전달하기에는 해킹의 문제를 고려하지 않을 수 없다.

본 논문에서는 이 문제를 해결하기 위하여 기존 사설망을 이용하여 멀리 떨어져 있는 여러 지사들과 하나의 사설망을 구축하는데, 각각의 지사에 데이터를 전송할 때는 인터넷을 통하여 전송하게 되나 이때 사설망에서 인터넷을 통하여 데이터를 전송시에는 타원 곡선 알고리즘을 이용하여 다른 알고리즘에 비해 빠른 시간에 암호화를 하여 정보를 전송하고 수신측에서는 암호화되어 들어온 정보를 복호화하는 기법을 제안한다.

2. 공개키 암호화 알고리즘

공개키 암호화 알고리즘은 두 개의 키 - 자신의 고유키(private key)와 상대방의 공개키(public key) -를 이용하여 정보를 암호화하는 기법으로 비 공개키 암호화 알고리즘에 비해 보안성을 보장할 수 있다.

[그림 1]은 공개키 암호화 알고리즘의 구성도이다.



[그림 1] 공개키 암호화 알고리즘 구성도

STEP 1 송신자가 메시지를 수신자에게 전달할 때 자신의 비밀키를 이용하여 암호화한다.

STEP 2 STEP 1에서 암호화된 메시지를 다시 수신자의 공개키로 암호화한다.

STEP 3 암호화된 메시지를 네트워크를 통해 수신자에게 전송한다.

STEP 4 수신자가 네트워크를 통해 메시지를 수신하면 송신자의 공개키로 복호화한다.

STEP 5 STEP 4에서 복호화된 메시지를 다시 수신자의 비밀키로 복호화한다.

공개키 암호화 알고리즘은 STEP 1에서 STEP 5까지의 수행으로 송신자의 메시지를 수신자만이 읽을 수 있는 형태가 된다

3 타원 곡선 알고리즘(Electric Curve Cryptographic)

Z_p 상의 타원 곡선 E는 다음과 같은 형태의 방정식으로 정의된다

$$y^2 = x^3 + ax + b \quad a, b \in Z_p \quad 4a^3 + 27b^2 \neq 0$$

0 을 무한점(point at infinity)이라 할 때 집합 $E(Z_p)$는

$E(Z_p) = \{ (x, y) \in Z_p \times Z_p \mid$ 위의 방정식이 성립 $\} \cup \{ 0 \}$

과 같이 나타낸다

■ 키 생성

1 Z_p상의 타원 곡선 E를 선택한 후 매우 큰 n을 선택한다 (∴ n은 $E(Z_p)$의 원소의 개수이다)

2 [1, n-1]사이에 있는 임의의 랜덤 수 d를 선택한다

3 Q = dP의 계산을 수행한다

4 개체의 공개키는 { E, P, n, Q }, 비밀키는 d이다

■ 암호화 과정

(B라는 사용자가 데이터 M을 A라는 사용자에게 전송한다)

1 A의 공개키 Q를 갖는다

2 데이터 M을 $m \in Fq$ 인 필드 요소로 표현한다

3 [1, n-1]의 사이에 존재하는 랜덤수 d를 선택한다

4 (x1, y1) = dP인 값을 계산한다

5 (x2, y2) = dQ인 값을 계산한다 만약 x2 = 0이면 3으로 간다

6 c = $m \cdot x2$를 계산한다

7 암호화된 데이터 (x1, y1, c)를 A에게 전송한다.

■ 복호화 과정

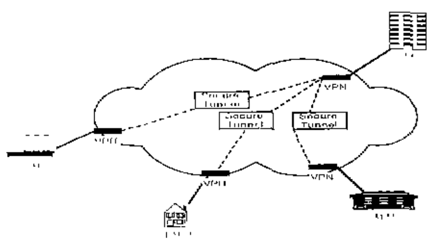
(A라는 사용자는 B로부터 전송 받은 암호문 (x1, y1, c)을 복호화한다)

1 A 자신의 비밀키 d를 사용해서 (x2, y2) = d(x1, y1)인 점을 계산한다

2 $m = c \cdot x_2^{-1}$을 계산해서 암호화하기 전의 데이터 m을 만든다

4 VPN(Virtual Private Network) 개념

VPN은 하나의 사설망을 한 곳이 아닌 여러 곳으로 나누어 관리할 수 있는 네트워크 솔루션으로 인터넷을 통신 네트워크로 사용하면서 기업의 보안이 필요한 정보를 주고 받을 수 있게끔 해 줄뿐만 아니라 전용회선을 위해 발생하는 여러 가지 추가 비용 부담을 줄여 줄 수 있는 네트워크 서비스이다 [그림 2]는 VPN의 간략한 구성도이다



[그림 2] VPN 구조

■ VPN의 필수 사항

① 호환성(Compatibility)

VPN에서 인터넷을 사용하기 위해서는, 사설망은 ISO(International Standards Organization) 3 계층의 IP(Internet Protocol)과 호환이 되어야 한다 가장 좋은 방법은 공식적으로 할당된 인터넷 주소를 사용하는 것이 좋다 하지만, 사설망에서 사용되는 주소는 공식적인 인터넷 주소가 아니기 때문에 적절하게 보안성을 갖춘 VPN을 이용하여 인터넷 네트워크를 이용하는 것이다. 사설망에서 인터넷을 사용할 때에는 적절한 보안 기능을 갖춘 시스템에서 주소를 변환하여 주고 또한 인터넷에서 사설망으로 들어가려는 할 때에도 적절하게 변환하는 장치가 필요하다

i 인터넷 주소로 변환 장치 - 사설망에서 사용되는 주소는 인터넷에서는 알지 못하는 주소이므로 인터넷을 이용할 수 있는 적절한 주소로 변환하는 장치이다

ii IP 게이트웨이 인스톨 장치 - 게이트웨이는 IP 주소를 다른 프로토콜로 변환하고 또한 역으로도 변환하는 작업을 수행(IP Authentication Header)한다

iii 터널링 기법 사용 장치 - 정보를 보낼 때 송신측에서 IP 패킷내의 다른 프로토콜 패킷들을 암호화하고 표준 IP 헤더를 첨가한다. 즉, 본 패킷은 payload이다 그런 다음 인터넷을 向여 목적지로 정보를 보낸다 수신측에서는 이 패킷을 다시 복호화하여 사용하는 기법이다

② 보안성(Security)

VPN을 구축할 때는 적절한 보안성 - 즉, 용도에 적절한 보안 기법 -을 제공하여야 한다 또한 관리하기에 쉬워야하고 사용자들에게는 투명성을 제공하여야 한다

가장 기본적인 보안 기법은 사용자 인증이다 즉, 각 사용자들에 대해 인증을 함으로서 인가되지 않은 사용자의 접근을 막고, 각 사용자는 지정된 사용자 영역에서만 작업을 수행할 수 있게 한다 또한 암호화기법을 사용하는 것이다. 인터넷을 통한 해킹 사건은 여러 차례 보도된바 있다 이를 해결하기 위해 암호화 기법을 이용하는데, iii 터널링 기법을 이용하면 제 3자 혹은 해커가 도청하는 행위를 하더라도 데이터를 볼 수 없기 때문에 안전하다

③ 이용성(Availability)

이용성은 가용 시간과 처리율을 강조하는데 사설망은 정해진 서비스 레벨을 보장한다 전용 회선은 회선을 사용할 수 있는 최대 능력으로 수행한다 반면 전화 회선에 의한 접근은 지역별에 의존적이다.

하지만 위에는 그와 같은 서비스 레벨은 존재하지 않는다 회선의 순간적인 폭주로 인한 경우일 지라도, 인터넷의 이용율은 거의 사설망에 의존한다 즉, 사설망의 이용 시간만큼 인터넷을 이용할 수 있다 처리율은 비용에 의해 결정된다 물론 인터넷의 폭주 시간에 사용하면 처리율도 떨어지지만 그보다는 인터넷을 사용하기 위해 어떤 장비를 사용하였는지에 따라 크게 네트워크의 처리율이 좌우된다

(4) 상호 운영성(Interoperability)

아직 뚜렷한 표준이 없기 때문에 각각의 통신상의 장애가 발생할 수 있다 즉, 상호간에 다른 VPN을 사용하였을 경우에는 서로 통신이 가능하지 않을 수도 있다 이를 위해 가능한 해결책은 동일한 판매자의 VPN을 사용하는 것이다 그렇지 않고서는 아직 완벽하게 사용할 수 없다

5 제안하는 알고리즘

본 논문에서 제안하는 시스템의 구성도는 [그림 3]과 같다

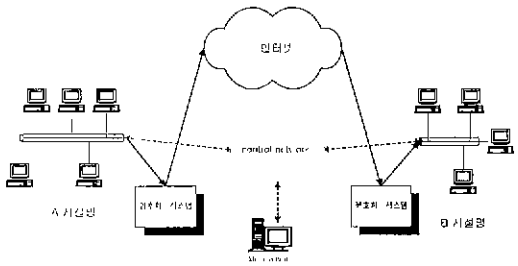


그림 3 제안하는 VPN 시스템

A 사설망과 B 사설망은 동일한 사설망으로써 멀리 떨어져 있다. 이때 A 사설망에서 B 사설망으로 인터넷을 통하여 데이터를 전송하고자 할 때 발생하는 패킷의 해킹의 문제를 해결하기 위해 각각의 시스템에서 패킷을 암호화하고 복호화를 수행한다.

[그림 4]는 암호화 및 복호화시에 수행되어지는 과정의 개략도이다

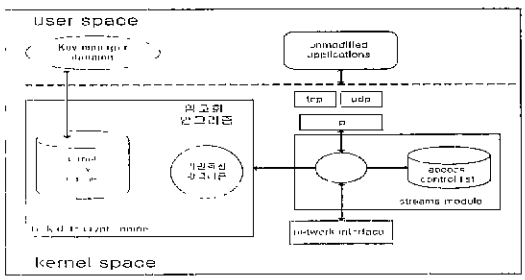


그림 4 암호화 복호화 개략도

A 사설망에서 제안하는 시스템을 통하여 데이터를 전송할 경우 제안한 시스템에 들어온 패킷은 transport layer까지는 다른 기존의 방법과 같이 패킷에 헤더를 첨가한다 하지만 network layer에서 IP 헤더를 첨가하기 전에 데이터 부분과 상호간에 서명부분 키인 authentication key를 패킷에 첨가하여 타원 곡선 암호화 알고리즘을 이용하여 암호화를 한 후 IP 헤더를 첨가하여 패킷을 전송한다

[그림 5]는 A 사설망에서 인터넷망으로 전송되어지는 패킷의 구조도이다

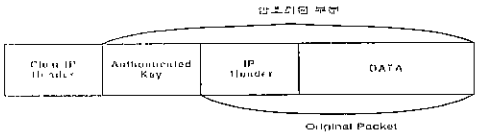


그림 5 패킷의 형태

[그림 5]의 패킷은 IP 헤더를 분석하여 해당 IP 주소에 전달된다 패킷을 전달받은 시스템은 먼저 암호화되지 않은 IP 헤더를 제거하고 어떤 시스템에서 보내진 것인지 검증을 한다 검증도 역시 타원 곡선 암호화 알고리즘을 이용하나 검증이 성공적으로 끝나면 상대방의 public key를 key manager daemon에서 가져와 복호화를 수행하고, 자신의 private key로 다시 한번 복호화를 하면 원래의 패킷 컴보를 볼 수 있다. 다음 IP 헤더 부분을 access control list와 비교하여 패킷의 허용 여부를 결정한다 허용된 주소라면 패킷은 사설망에 있는 해당 호스트로 패킷을 무사히게 전송할 수 있다.

key manager daemon은 [그림 6]과 같은 레코드로 구성되어진다

```
record is
    remote IP address
    remote Public value
    own public value
    own private value

end record
```

그림 6 Key Management Daemon 레코드

[그림 6]처럼 key manager daemon은 데이터를 암호화하고 복호화할 때 필요로하는 키 부분들을 유지하고 있다 buck data crypt engine에서 실질적으로 서비스들을 암호화하고 복호화하는 부분이다. 마지막으로 streams module은 buck data crypt engine의 클라이언트이다 인터넷에서 들어온 패킷은 복호화가 끝나면 원래 패킷의 IP 헤더 부분과 access control list부분을 참조하여 허용 가능한 패킷인지 아닌지를 확인한다 만일 사설망에서 들어온 패킷이라면 자신의 서명 부분을 첨가하여 모두 암호화가 된 데이터를 받아 IP 헤더를 첨가한 뒤 네트워크 인터페이스를 통해 패킷을 전송할 수 있도록 한다

6. 결 론

본 논문에서는 하나의 사설망이 여러 지역으로 분산되어 있는 경우 VPN 기법을 사용하여 기존의 사설망에서 문제시되었던 전용선의 비용이나 보안의 문제점을 해결하였다 또한 암호화 기법으로 기존의 RSA와 같은 암호화할 때 걸리는 약간의 오버헤드도 최소한으로 줄여 보다 효과적으로 네트웍이 가능하도록 하였다.

향후 방향은 제시한 VPN은 상호 이종간의 처리는 고려하지 않았기 때문에 모든 패킷에 대하여 처리하기가 어렵다 이 문제점은 현 VPN에 각각의 clear, secure, optionally secure한 패킷들을 구별하여 처리할 수 있도록 해야 한다

7. 참 고 문 헌

[1] Elliptic Curve DSA(ECDSA). An Enhanced DSA. Don B Johnson, Alfred J Menezes

[2] T ElGAMAL, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, 1985

[3] N Koblitz, "Elliptic Curve cryptosystems", 1987

[4] A Menezes, Elliptic curve public key cryptosystems Kluwer, 1993

[5] SKIP - Securing the Internet, Germano, Hannos Lubich, Ashar, Tom Markson, Rich Skrenta

[6] Design and Implementation of SKIP, Ashar Aziz, Martin Patterson, ICG-95-0004, 1995

[7] W R Cheswick, S. M Bellovin, "Firewalls and Internet Security", Addison-Wesley, 1994

[8] Virtual Private Networks Resource Guide