ESP 프로토콜에서의 문제점 보완 알고리즘

이 영 지[†] · 김 태 윤[††]

요 약

IPSec은 공용 네트워크 상에서 암호화와 인증, 무결성을 제공하기 위해 사용되는 프로토콜이다. IPSec에서는 전송되는 패킷에 암호화와 인증, 무결성을 추가해 전달하기 위해 ESP 프로토콜을 사용한다. ESP는 패킷 암호화를 위해 DES-CBC 알고리즘을 이용하는데 이 모드에서는 ESP 프로토콜로 보호되어 전송되는 데이터를 암호화하기 위한 초기 값으로 IV(Initialization Vector) 값을 사용한다. 이 값은 수신 측의 패킷 복호화를 위해 공개적으로 전달되므로 중간에 공격자에 의해 공격당할 위험이 많다. IV의 값이 조금이라도 변경되면 ESP의 모든 데이터의 복호화가 이루어지지 않고 상위 레벨의 정보가 변경되는 등 심각한 문제가 발생한다. 이것은 보안을 목적으로 하는 IPSec에서는 치명적인 약점이 될 수 있다. 따라서 본 논문에서는 ESP 프로토콜에서의 문제점인 IV를 안전하게 전송하기 위한 새로운 알고리즘을 제시한다. 이 방법은 IV 값은 DES-ECB 알고리즘을 이용하여 암호화하여 IV 공격을 방어하고 메시지 인증 함수를 추가 적용하여 ESP 전체 데이터의 무결성 체크도 가능하게 한다. 제안된 알고리즘으로 IV와 데이터에 대한 공격을 방어할 수 있고 안전한 전송을 보장한다.

The problem resolution algorithm in ESP protocol

Young-Ji Lee[†] · Tai-Yun Kim[††]

ABSTRACT

IPSec is a protocol which provides data encryption, message authentication and data integrity on public and open network transmission. In IPSec, ESP protocol is used when it needs to provide data encryption, authentication and integrity in real transmission packets. ESP protocol uses DES-CBC encryption mode when sender encrypts packets and receiver decrypts data through this mode IV is used at that time. This value has many risks of attack during transmission by attacker because it is transferred clean and opened. If IV value is modified, then decryption of ESP data is impossible and higher level information is changed. In this paper we propose a new algorithm that it encrypts IV values using DES-ECB mode for preventing IV attack and checks integrity of whole ESP data using message authentication function. Therefore, we will protect attacks of IV and data, and guarantee more safe transmission on the public network.

키워드 : IPSec, IV, ESP, DES-ECB, DES-CBC, 메세지 인증(Message Authentication), SA

1. 서 론

최근 네트워크의 데이터 전송에 대한 중요도와 관심이 커져가고 있다. 공개적인 네트워크를 통해 대량의 자료가 전송되고 온라인 상으로 보안이 필요한 자료가 많이 전달됨에 따라 네트워크에 대한 보안과 신뢰성이 중요시되고 있다. 이에 따라 전송되는 정보를 안전하게 보호하기 위해 패킷을 암호화하거나 보안을 제공해주는 프로토콜과 방법이 많이 이용된다.

IPSec(Internet Protocol Security)은 IP와 그 상위 계층(예를 들면, UDP, TCP)에 대해 보안을 제공하는 프로토콜이다. IPSec은 공개적인 인터넷의 네트워크 계층에서 패킷을 주고받을 때 메시지에 대한 암호화, 인증, 무결성 등의 기능을 제공한다[2, 16].

IPSec에서 주된 역할을 하는 두 프로토콜은 패킷에 인증과 무결성을 제공하는 AH(Authentication Header)와 AH에서 제공하는 기능 외에 암호화를 추가 제공하는 ESP(Encapsulating Security Payload)이다[3, 6].

IPSec이 전송되는 데이터에 대해 보안 기능을 제공하는 만큼 데이터 전송중에 IPSec을 공격하려는 시도도 많이 일어난다[4]. IV(Initialization Vector)는 ESP에서 쓰이는 암호 알고리즘인 DES-CBC 모드에서 데이터에 대한 암호화를 제공할 때 사용되는 초기 값이다[5].

ESP의 처음 패킷은 IV와의 XOR을 통해 암호화가 이루어진다. 수신 측에서는 ESP 패킷을 받은 다음 IV를 이용하여 패킷을 복호화한다. IV는 ESP 패킷의 페이로드 부분에 포함되지만 수신 측이 IV를 이용해 암호화된 데이터를 다시 복호화하기 위해서 IV 값은 암호화되지 않고 그대로 노출되어 공개적으로 보내진다. 따라서 전송상의 위험이 많아지는데 IV

† 준 회 원 : 고려대학교 대학원 컴퓨터학과
†† 종신회원 : 고려대학교 컴퓨터학과 교수
논문접수 : 2001년 8월 17일, 심사완료 : 2001년 11월 21일

의 값이 조금이라도 변경되면 수신 측에서의 복호화가 불가능하고, 경우에 따라 그 상위 레벨의 정보까지 변경되는 등 심각한 문제가 발생한다. 이 같은 문제는 데이터의 보안과 암호화를 제공하는 IPSec에서 커다란 취약점이 된다. 따라서 이렇게 IV를 변경시켜서 일어나는 IV 공격(IV attack)을 방어하기 위한 많은 연구가 진행되고 있다[4].

본 논문에서는 IPSec에서의 IV 공격을 방어하기 위한 방법을 제시한다. 제시하는 알고리즘은 노출된 상태로 전송되는 원래의 IV 값에 DES-ECB 모드를 적용하여 암호화하고, IV를 포함한 ESP 전체 페이로드 부분에 메시지 인증 함수를 적용하는 것이다. 수신 측에서는 패킷을 받은 다음 메시지 인증 함수를 통해 데이터 전체에 관한 무결성도 체크할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 IV 공격에 대한 내용과 ESP 헤더, 그리고 기존의 IV 공격 방지에 관한 연구들을 분석한다. 3장에서는 본 논문에서 제시하는 DES-ECB 암호화를 이용한 IV 공격 방어 알고리즘과 메시지 인증 함수를 이용한 데이터 무결성 체크에 관한 알고리즘을 설명한다. 4장에서는 알고리즘의 성능을 평가하고 기존의 IV 방어 알고리즘과 보안 알고리즘이 만족해야 하는 몇 가지 항목에 대해 비교 분석을 하고 5장에서 결론과 향후 과제를 제시한다.

2. 관련 연구

본 장에서는 본 논문에서 제시하는 알고리즘을 제안하게 된 동기와 그에 관련되어 진행된 관련 연구와 기존의 연구 방법들을 살펴본다.

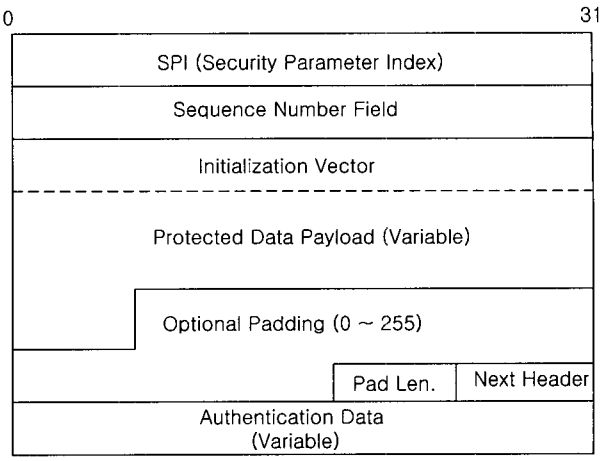
2.1 ESP(Encapsulating Security Payload)

IPSec의 주된 프로토콜은 AH와 ESP이다. AH는 IP 페이로드에 인증과 무결성을 제공하고, ESP는 데이터의 인증과 무결성 체크와 함께 데이터 암호화를 제공한다[2].

ESP는 전송되는 데이터에 암호화를 제공하기 위해 기본적으로 DES 알고리즘을 사용한다. 송신 측이 암호화된 페이로드를 IV와 함께 전송하면 수신 측은 IV와 그 전 패킷을 XOR하고 복호화 알고리즘을 사용하여 데이터를 복호화한다[3].

(그림 1)은 ESP 헤더의 구조이다. 보호된 페이로드 데이터 안에 IV가 포함된 것이 나타나 있다. 각각의 데이터는 고유의 IV를 포함하고 있고 이것은 데이터가 전송되는 중간에 유실되거나 패킷 순서가 다시 정해지는 경우에도 해당 데이터를 안전하게 복호화할 수 있음을 보장한다[1].

페이로드는 DES-CBC로 안전하게 암호화되어 전송되지만 IV는 송신 측에서 전송된 IV 값을 사용해 암호화된 ESP 데이터를 복호화해야 하기 때문에 암호화되지 않고 공개적으로 전송된다. 이 단계에서 공격당할 위험이 많아지는데, 중간에서 공격자에 의해 IV 값의 일부가 바뀌면 수신자는 ESP 데이터를 복호화하지 못할 뿐 아니라 프로토콜의 구조에 따라 상위 레벨의 정보까지 바뀔 수 있다.



(그림 1) ESP 헤더 구조

IV를 포함한 데이터가 변경되면 수신자는 전송된 데이터를 신뢰하지 못하고 잘못된 변경 데이터를 사용하는 등 심각한 문제가 발생한다. IPSec은 공용 인터넷망을 통해 전송되는 데이터에 무결성과 암호, 인증 등을 제공하는 프로토콜이므로 IV 공격은 커다란 취약점이 된다. 이런 문제점을 해결하기 위해 IV 공격을 방어하기 위한 여러 가지 방법에 대한 연구가 진행되고 있다[1].

2.2 IKE(Internet Key Exchange)

SA(Security Association) 협상은 통신 개체가 서로에 대해 인증을 하고 통신 연결을 맺어 보호된 데이터를 보내기 위한 준비 단계이다. 이 단계는 IKE를 통해 자동적으로 이루어진다. IKE는 두 단계로 구성되며 AH나 ESP 헤더에 의해 보호된 데이터를 전송하기 위해 그 전에 두 통신 개체 사이의 패킷 보호 프로토콜, 암호화 알고리즘, 전송 형태, 키 값들, 키들의 생명 주기(life time) 등 실제 데이터를 보내기 전에 결정되어야 할 것들을 협상한다.

첫 번째 단계에는 메인 모드(main mode)와 어그레시브 모드(aggressive mode)가 정의되고 ISAKMP(Internet Security Association Key Management Protocol)를 통해 키 값들의 교환을 위한 통신 개체간의 통신 환경들을 설정한다[18].

1단계가 완료되면 통신 개체간의 환경 설정이 끝나고 IPSec을 이용한 통신을 위한 두 번째 단계의 SA 협상 과정이 시작된다. 1단계에서 통신 개체 인증과 그에 따른 필요한 절차들이 설정되었으므로 두 번째 단계는 퀵 모드(quick mode)라고 불리우는 간략화된 형태로 협상이 이루어진다. 2단계가 종료되면 서로의 통신 개체 사이의 인증 절차와 필요한 알고리즘, 키 값 협상이 완료되고 실제 데이터의 전송이 시작된다. 본 논문에서 제시하는 DES-CBC 모드의 키 값과 메시지 인증 함수에 대한 협상은 두 번째 단계인 퀵 모드에서 이루어진다.

2.3 IV 공격(Initialization Vector Attack)

IV 공격은 IPSec에서 적용한 블록 암호 알고리즘인 DES

(Data Encryption Standard)의 CBC(Cipher Block Chaining) 모드에서의 공격이다. 이 공격은 중간에서 공격자가 CBC 암호에서 인증되지 않은, 즉 변경된 IV를 사용한다. 수신 측에서는 공격자가 변경해놓은 IV로 인해 복호화가 불가능하거나 변경된 정보를 사용하는 문제가 발생한다.

DES-CBC 모드는 블록 단위별로 데이터를 암호화한다. 블록 암호의 CBC 모드에서 암호화되는 데이터는 평문 블록으로 나누어진다. 그것을 $P_1, P_2, \cdots$, 로 표현한다면 평문 블록은 다음과 같은 수식에 의해 암호화된다.

$$C_i = f_k(P_i \oplus C_{i-1})$$

그리고 다음과 같이 반대 과정을 통해 복호화된다.

$$P_i - f_k^{-1}(C_i) \oplus C_{i-1}$$

여기서 fk와 fk^{-1}은 각각 블록 암호의 암호화와 복호화를 나타낸다. 그리고 '⊕'는 XOR이다. 현재 데이터는 이전 데이터의 값으로 XOR하여 암호화되는데 첫 번째 블록에는 XOR할 이전 데이터 값이 없다. 이 때 IV 값이 사용된다[7].

IV는 보통 송신자에 의해 무작위로 선택되고 암호화된 메시지와 함께 또는 그 전에 전송된다. IV는 다음과 같은 수식에 의해 암호문을 복호화한다.

$$C_1 = f_k^{-1}(P_1 \oplus IV)$$
$$P_1 = f_k^{-1}(C_1) \oplus IV \quad (1)$$

만일 IV가 인증 작업에 의해 보호되지 않거나 노출되어 전송된다면 공격자는 IV를 쉽게 변경할 수 있게 된다. 그렇게 되면 식 (1)에 따라서 복호화된 데이터의 첫 번째 블록도 변경할 수 있다. 첫 번째 블록에는 여러 가지 헤더 정보들이 포함되기 때문에 변경된 데이터는 인증되지 않은 데이터의 사용으로 수신 측에 피해를 준다. 만일 암호화가 프로토콜 스택의 중간 단계에서 이루어진다면 첫 번째 블록은 상위 레벨의 헤더에 관한 내용까지 포함하고 그 값들이 변하기 때문에 심각한 결과를 초래한다.

모든 IPSec은 CBC 모드에서의 블록 암호를 사용하기 때문에 IV 공격은 암호에서도 커다란 문제가 되며 이 알고리즘의 대부분은 인증되지 않은 IV를 사용한다[1].

IV에 대한 공격은 ESP 헤더로 보호된 데이터가 공용 네트웍 망을 통해 전송될 때 발생한다. ESP 헤더 안에 포함된 IV와 데이터 페이로드는 함께 전송되지만 암호화된 데이터와는 다르게 IV 값은 암호화되지 않고 노출된 상태로 전송되므로 공격자는 패킷에 접근하여 IV 값을 쉽게 변경시킬 수 있다.

위와 같은 여러 문제점들 때문에 IV를 보호하고자 하는 방법들이 제안되었고 본 논문에서는 IV 공격을 방어하는 방법에 대한 새로운 알고리즘을 제시한다.

2.4 IV 공격 방어에 대한 기존의 연구 분석

IV의 공격을 막기 위한 방법은 아래와 같이 여러 방향으로 연구되었다. 첫째, 데이터를 보낼 때마다 실제 IV의 값에 단방향 해쉬 함수(one way hash function)를 적용하여 해쉬된 값을 넣어 전송하는 방법이 있다. 해쉬 함수는 임의의 크기의 데이터를 입력받아 해쉬 함수를 적용하여 일정한 크기의 출력 값을 내는 함수이다. IV를 포함한 전체 데이터들을 단 방향 함수로 해쉬하고 결과 값을 인증 데이터 필드에 저장하여 전송한다. 수신 측에서는 데이터를 받고 송신 측이 사용한 것과 같은 해쉬 함수를 이용해 해쉬하여 결과 값을 비교한다. 만일 IV가 변경되었다면 해쉬의 결과 값이 다르게 나타나므로 무결성 체크를 통해 변화 여부를 알 수 있다. 하지만 이 방법은 IV 공격이 일어났을 때 수신 측에서 IV의 인증 여부만 알 수 있다는 한계가 있다[1]. IPSec에서는 기본적으로 128 비트의 해쉬 값을 내는 MD5 함수와 SHA-1을 사용한다. 해쉬 알고리즘에 입력 값으로 IV를 포함한 ESP의 전체 데이타 필드를 입력하여 해쉬 값을 계산한다. 계산된 결과 값을 ESP 헤더의 마지막 부분에 있는 인증 데이터 필드 부분에 포함하여 전송한다. 해쉬 함수는 일반적으로 인증에 사용되므로 수신 측에서 받은 IV 값을 해쉬 함수를 돌려 같은 결과 값이 나오면 인증된 것으로 간주한다. 이 때 사용되는 해쉬 함수는 미리 두 통신 개체간에 정의되어 있어야 한다. 하지만 이 방법은 단순히 메시지 인증 함수에 해쉬 함수를 사용한 것과 같기 때문에 그 이상의 결과를 기대하기 힘들다.

둘째, IV의 값을 다양하게 변화시키는 방법이다. CISCO에서는 IV 값을 전송할 때마다 IV의 값을 4비트 또는 8비트로 바꿔 가면서 데이터와 함께 전송하는 방법에 관한 연구를 하고 있다. 이 때 사용되는 IV의 기본 값은 8비트이다. 이 알고리즘은 IV 값에 대한 옵션을 주어서 옵션을 선택하지 않으면 8비트로 전송되고 옵션을 선택하면 4비트로 전송되도록 한다. 이 방법은 보내기 전에 보내는 송신자와 수신자 사이에 어떤 크기의 IV를 보낼 것인지에 관한 약속이 이루어져 있어야 한다. 그 약속에 따라 정해진 길이의 IV를 보낸다. 이 방법은 아직까지 두 종류의 정해진 길이밖에 사용을 못하고 또 보내는 쪽에서 임의로 IV의 값을 선택할 수 없다는 단점이 있다[15]. 따라서 보낸 값의 길이가 다르면 그 값은 수신 측에서 사용하지 못하고 그대로 폐기되어야 한다.

셋째, DES-CBC 암호를 사용하여 IV를 암호화하는 방법과 0과 같은 변수 기반의 IV를 사용하는 방법이 있다. CBC 모드를 사용하여 IV를 암호화하는 것은 CBC 모드를 다시 적용하는 것으로 또 다른 IV 초기 값이 생기는 모순을 만든다. 그리고 DES로 암호화를 했을 때 다시 생기는 IV의 전송 방법도 문제시된다. 이런 방법은 IV를 안전하게 전송하기 위한 적절한 방법이 될 수 없다[1].

따라서 본 논문에서는 IV 공격을 방지하는 새로운 방법을 제시하고자 한다. 제시하는 알고리즘은 DES-ECB 모드를 사용하여 IV 값을 암호화하고, ESP 헤더 값에 메시지 인증 함수를 사용해 무결성을 체크하는 인증 데이터(Authentication Data) 부분을 기본적으로 제공한다. 그 부분에 메시지 인증 함수 값을 삽입해 전송함으로써 암호화와 데이터의 무

결성 체크를 동시에 수행한다.

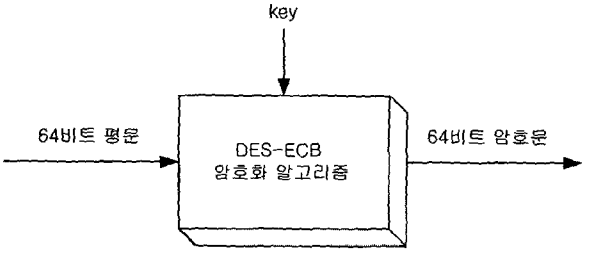
3. 안전한 IV 전송을 위한 제안 알고리즘

본 장에서는 IV 공격을 방어하기 위해 DES-ECB 암호를 적용해서 보안을 강화하고, ESP 헤더와 페이로드 전체 값에 메시지 인증 함수를 적용한 값을 함께 전송해 무결성을 보장하는 알고리즘에 대해 설명한다.

3.1 DES-ECB 알고리즘을 이용한 IV 암호화

본 논문에서는 ESP의 페이로드 부분에 있는 IV를 암호화하기 위해 DES-ECB 모드를 사용한다. ECB 모드는 DES 알고리즘에서 가장 간단한 모드로 64비트의 입력을 받아 64비트의 키 값을 이용하여 그대로 암호화하여 64비트의 암호문을 만드는 방법이다. 본 논문에서 ECB 모드를 사용하는 이유는 이 알고리즘이 가장 간단하여 복호화도 쉽고 빠르며 다른 모드와 달리 또 다른 부가적인 IV를 필요로 하지 않기 때문이다. 만일 DES-CBC 모드를 사용하면 IV를 암호화하기 위해 또 다른 IV를 필요로 하는 모순이 생긴다. 이에 비해 간단한 ECB 모드를 사용하더라도 IV를 공격자로부터 보호하기 때문에 보안을 유지할 수 있다.

IV의 길이는 32비트의 배수(multiple) 값 안에서 다양한 크기를 가진다. 32비트와 64비트가 주로 쓰이는데 본 논문에서는 DES-ECB 모드를 사용하기 위해 IV의 크기는 64비트라고 정의한다. (그림 2)는 DES-ECB가 동작하는 과정을 나타낸다[12].



(그림 2) DES-ECB 암호화 과정

암호화된 IV 값은 ESP의 헤더의 IV 필드 위치에 삽입되어 전송된다. 이 알고리즘으로 IV를 암호화하면 그 값이 캡슐화 되어 외부에서는 실제 IV 값을 보지 못한다.

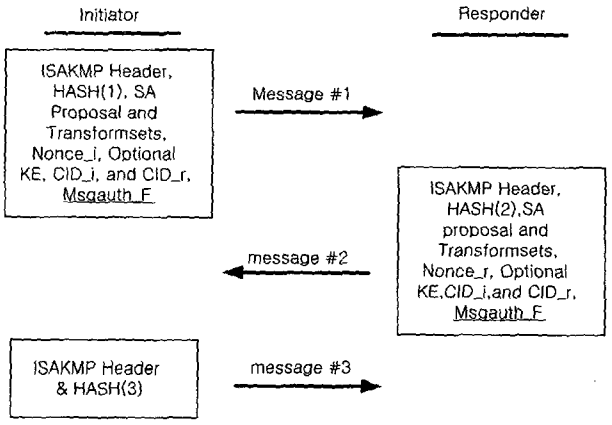
ECB 모드를 적용하여 IV를 암호화 할 때 사용되는 키 값의 크기는 64비트이다. 이 값은 SA 단계에서 협상되어야 하지만 본 논문에서는 SA 단계에서 DES-ECB 모드의 키 값을 따로 협상하는 부하를 줄이기 위해 DES-CBC 모드에서 협상했던 키 값을 그대로 사용하기로 한다. DES-CBC의 키 값을 그대로 사용하면 DES-ECB 키를 따로 협상해야 하는 부하를 줄일 수 있을 뿐만 아니라 키 값을 저장하는 공간과 키 값을 찾는 부가적인 순서가 필요 없게 된다.

ECB 모드를 이용해 IV를 암호화하고 ESP 페이로드와 그 안에 포함된 IV에 대한 메시지 인증을 적용하여 데이터와 IV의 무결성을 체크하는 방법을 함께 제공한다.

3.2 IKE의 SA 협상 단계에서의 메시지 인증

IKE를 이용한 SA 협상 단계에서는 AH나 ESP 헤더로 보안된 데이터 전송을 위한 여러 가지 사항들을 결정한다. 이때는 IKE(Internet Key Exchange)를 이용하여 자동적으로 설정하고 송수신 개체간의 정책 설정이 기본이 된다. IKE는 보안 정책들을 협상하는데 IPSec에서는 기본적으로 메시지 인증 함수를 위해 HMAC-SHA1, HMAC-MD5 함수를 사용한다. 메시지 인증 함수들은 IKE에서 통신 개체간의 협상을 통해 두 송수신 개체 사이의 환경과 정책에 따라 자동적으로 설정되고 송수신 개체나 사용자는 결정되는 인증 방식에 대해 관여하지 않는다[9].

아래의 (그림 3)과 같이 SA 단계에서는 여러 가지 협상 항목들이 전송된다. 그림은 이 중에서 두 번째 퀵 모드에서의 협상 사항을 나타낸다.



(그림 3) 퀵 모드의 키 값 협상 과정

1단계에서 정의된 보안 정책은 2단계에서 퀵 모드를 통해 구현된다. IKE의 모든 단계에서 전송되는 메시지는 SKEYID_e와 SKEYID_a를 통해 암호화되고 인증된다.

송신 측(Initiator)에서 제안 사항이 포함된 여러 가지 패킷을 보내면 수신 측(Responder)에서는 제안된 사항들 중에서 수신 측의 알고리즘과 대응하는 알맞은 알고리즘과 키 값들을 결정하여 송신 측에게 되돌려 보내는 것으로 협상이 이루어진다[22].

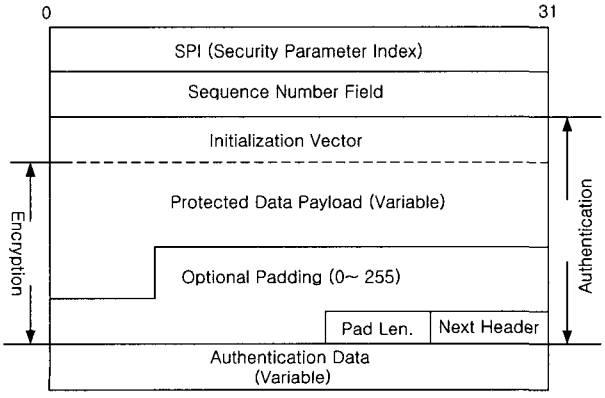
송신 측에서 보내는 패킷들은 ISAKMP 헤더와 HASH 페이로드(HASH 페이로드에는 어떤 옵션들이 선택되어졌는지에 관한 속성들이 포함된다), SA 제안 사항과 전송 형태를 나타낸 SA 제안과 전송 형태(SA Proposal and Transformsets), 재전송 공격 방지를 위한 난수 값(Nounce_i), 통신 개체가 AH나 ESP에서 데이터 암호화를 위해 대칭 키를 생성할 때 사용되는 Diffie-Hellman 공개키가 포함되는 선택적인 키 교환(Optional KE), 클라이언트 ID인 CID_i와 CID_r 등이 포함된다. 송신 측이 제안 사항들과 키 값을 보내면 수신

측에서는 올바른 송신 측에서 온 데이터인지 확인하고 제안된 사항 중에서 수신 측에서의 사항과 부합되는 알고리즘을 선택하고 그 밖의 사항들을 결정해 송신 측에게 보낸다. 송신 측도 올바른 수신 측에게서 온 데이터인지 인증 하고 패킷을 잘 받았다는 확인 응답(acknowledge)을 보냄으로서 SA의 퀵 모드가 완료되고 두 통신 개체는 본격적으로 AH나 ESP로 보호된 데이터 전송을 시작한다.

본 논문에서는 이 교환 단계에 메시지 인증을 위한 함수(msgauth_F)를 추가하고 ESP의 인증 데이터(Authentication Data) 필드를 정의한다. (그림 3)의 첫 번째, 두 번째 메시지 교환에서 Msgauth_F 부분이 본 논문에서 추가한 함수 값이다. 메시지 인증 함수를 추가하기 위해 SA 협상 단계의 퀵 모드에서 메시지 인증 함수에 관한 알고리즘과 키 값, 함수들을 교환한다. 본 논문에서는 SA 협상 단계에서 이 항목을 기본 설정 값에 포함시킨다. IKE는 두 통신 개체 사이에서 요구하는 사항들을 분석하여 알맞은 메시지 인증 단계를 설정한다. 함수에 필요한 키 값들은 IKE 단계에서 자동적으로 설정되고 SADB에 저장되어 전송된 데이터들을 인증할 때 사용된다. 메시지 인증 함수는 SA 단계에서 IKE에 의해 자동적으로 결정되지만 IPSec에서는 HMAC 함수를 기본적으로 제공한다[19].

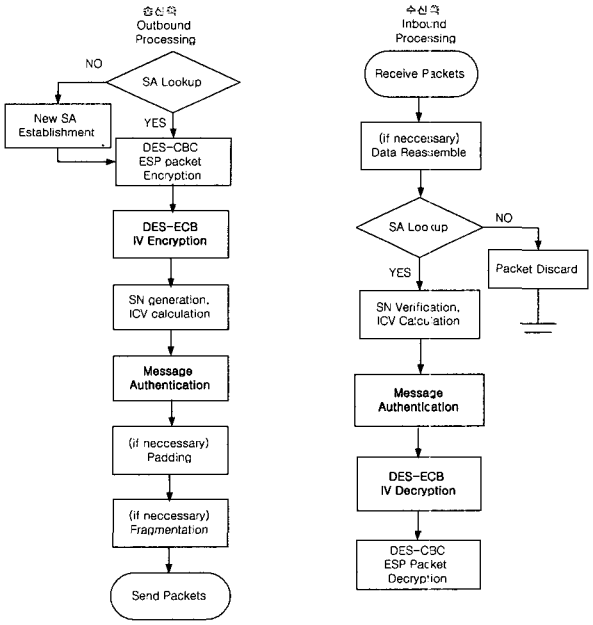
3.3 전체적인 알고리즘

(그림 4)는 암호화와 메시지 인증이 추가된 ESP 헤더를 나타낸다. ESP의 데이터 페이로드와 IV는 각각 다른 알고리즘을 사용해 암호화된다. 먼저 IPSec에서 제공하는 암호화 과정에 따라 ESP의 데이터 페이로드가 DES-CBC 모드를 이용해 암호화되고 여기에 본 논문에서 제시하는 DES-ECB 모드를 이용한 IV 암호화 과정이 추가된다. 암호화된 IV 값은 IV 필드에 저장되어 전송되고 IV를 포함한 전체 데이터에 메시지 인증 함수를 적용한 값을 인증 데이터 필드에 저장한다. 수신자는 복호화 알고리즘을 통해 암호화된 원래 IV의 값을 복원하고 그 값을 이용해 ESP 헤더를 복호화한다. 그리고 메시지 인증 함수를 통해 데이터의 무결성을 확인한다.



(그림 4) ESP 헤더의 암호화와 인증 부분

다음 (그림 5)는 본문에서 제시한 알고리즘의 전체적인 흐름도이다. 아래와 같은 과정으로 알고리즘이 진행된다.



(그림 5) 전체 알고리즘 흐름도

두 통신 개체가 IKE를 이용한 SA 협상을 완료하면 실제 패킷에 ESP 헤더를 붙여 기밀성을 유지한 데이터 전송을 시작한다. (그림 5)는 SA를 완료하여 두 통신 개체 사이의 연결이 이루어진 후의 전체 알고리즘을 나타낸다.

송신 측에서는 우선 SPI(Security Parameter Index)를 이용해 SADB에서 그 전 단계에서 설정된 알맞은 SA를 찾는다(SA Lookup). 만일 설정된 SA가 없으면 정책에 따라 새로운 SA를 설정한다(New SA Establishment). SA를 찾았으면 ESP를 통해 전송될 데이터를 DES-CBC 모드를 적용하여 암호화하고(DES-CBC ESP Packet Encryption), 그 다음 본 논문에서 제안하는 DES- ECB 모드를 이용한 IV 값의 암호화가 일어난다(DES-ECB IV Encryption). 재전송 공격 방지를 위해 일련 번호를 생성한다(SN generation). 이 값은 패킷 순서에 따라 순차적으로 증가하는 값이다. 이 값을 체크하여 중간에 유실된 패킷을 알아낼 수 있다. 이 때 SN의 초기 값은 '0'이다. 다음으로 전송 중 변하지 않거나, 수신 측에서 예측 가능한 필드 값을 이용해 데이터의 무결성 체크를 위한 ICV 계산이 이루어지고(ICV Calculation) 본 논문에서 추가한 메시지 인증 함수를 적용한다(Message Authentication). 최종적으로 필요한 경우에 패딩(Padding)을 추가한 후 전송할 패킷 단위로 일정하게 분할하는 단편화 작업이 수행된다(Fragmentation). 마지막으로 패킷을 수신 측으로 전송한다(Send Packets).

수신 측에 의해 보안 유지되어 전송된 패킷이 수신 측에 도착하면 송신 측과는 반대의 작업이 진행된다(Receive Packets).

수신된 패킷 중에 분할된 패킷이 있으면 재조합하고(Date Re-assemble) ESP 헤더의 {SPI, ESP, destination address}를 이용하여 관련된 SA를 찾는다(SA Lookup). 만약 설정된 SA가 없는 경우에는 해당 패킷을 폐기한다(SA Discard). 수신 측에서는 SA를 찾는 단계뿐만 아니라 매 단계에서 결과 값과 패킷의 값이 일치하지 않으면 패킷을 폐기한다. 수신 측에 설정된 SA가 있으면 슬라이딩 송신 윈도우(Sliding Receive window)와 비트 매스킹(Bit Masking)을 이용하여 SN과 ICV에 관한 검증을 수행하고(SN Verification, ICV Calculation) ICV 검증 단계에서 수신 패킷 내의 ICV 값이 ESP 내의 값과 일치하면 통과시키고, 그렇지 않으면 해당 패킷을 폐기한다. 본 논문에서 제시하는 메시지 인증 함수를 이용하여 메시지의 무결성을 체크하고(Message Authentication) DES-ECB로 암호화된 IV를 복호화한다(DES-ECB IV Decryption). 복호화된 IV를 이용해 DES-CBC 모드로 암호화된 데이터 페이로드를 복호화하고(DES-CBC ESP Packet Decryption) 수신 측에서의 나머지 작업을 수행한다.

IPSec에서 기본적으로 제공하는 메시지 인증으로는 SN과 ICV 검사가 있다. 본 논문에서는 데이터 안전과 기밀성을 좀 더 강화시키기 위하여 기본 방법에 메시지 인증 함수를 추가하였다. SA 단계에서 협상한 메시지 인증 함수를 SN, ICV 검사 뒤에 적용하여 수행한다. 송신 측에서는 암호화를 먼저 한 다음 전체 메시지에 대한 인증을 하고 수신 측에서는 메시지 인증 함수를 적용하여 그 데이터들이 올바른지 확인한 다음에 데이터 복호화를 한다.

4. 알고리즘 성능 평가 분석

4.1 알고리즘 분석

본 논문에서는 기존 IPSec의 문제점 중의 하나인 IV에 대한 공격을 방지하는 해결책을 제안하였다. 제안된 알고리즘은 특별히 다른 함수를 사용하지 않고 IPSec에서 기본적으로 적용하는 암호 알고리즘과 메시지 인증 함수를 적용한다. SA 단계에서 설정된 키 값과 알고리즘을 이용하여 부가적인 오버 헤드가 거의 발생하지 않고 IV에 효과적인 암호화와 메시지 인증의 추가적인 기능을 제공하는 방법에 중점을 두었기 때문에 빠른 수행 시간과 적은 비용, 호환성을 장점으로 가진다.

본 논문에서는 IV 값에 DES-ECB 암호를 적용하여 데이터의 기밀성을 제공하고 메시지 인증 함수를 적용해 데이터의 무결성을 보장한다. 메시지 인증 함수는 두 통신 개체의 SA 단계에서 IKE를 통해 자동적으로 결정된다. 제시한 알고리즘을 통해 IV 공격을 받았을 때 수신 측에서 복호화가 불가능하고, 잘못된 데이터를 사용하는 등의 문제점을 해결하고 안전한 전송을 보장한다.

다음은 본 논문에서 쓰인 암호화 방법이다.

DES-ECB 모드는 64비트의 블록으로 나누어서 각 블록별로 독립적인 DES 암호화를 수행한다. 평문 m이 64비트의 블록 $m1, m2, m3, \cdots$와 같이 나누어질 경우,

$$ECB\ 암호화 : C_i = Ek(m_i),\ i = 1, 2, 3, \cdots$$
$$ECB\ 복호화 : m_i = Dk(C_i)$$

이와 같은 방식으로 암호화가 이루어진다. IV의 암호화된 값을 받은 수신 측에서는 위의 복호화 방법을 이용하여 원래의 IV 값을 복원한다. 이 방법은 간단하지만 중간에서 공격자가 IV 값을 보지 못할 정도의 보안성을 제공한다. 이 모드에는 동일한 비밀키가 연속해서 사용되는 경우에는 비슷한 복호화 문이 나온다는 점과 동일한 평문 블록은 동일한 암호문 블록으로 암호화되는 취약점을 가진다. 하지만 이 점은 IV 값이 매 패킷마다 변화하므로 충분히 보완된다[15].

4.2 기존의 IV 공격 방어 알고리즘과 비교 평가

이번 장에서는 기존의 다른 IV 공격 방어 연구와 본 논문에서 제시하는 IV-DES 암호화와 ESP 헤더에 메시지 인증 함수를 추가한 방법을 비교 분석한다.

<표 1>에서 보는 것과 같이 기존의 연구와 본 논문에서 제시하는 알고리즘을 몇 가지 항목에서 비교하였다. 4가지 항목은 보안을 목적으로 하는 알고리즘에서 기본적으로 제공해야 하는 항목이다. 기존 연구에서 IV 크기 변환과 해쉬 함수는 한 가지 방법만 적용했기 때문에 모든 공격을 방어하지 못한다. 나머지 한가지 연구 방법인 DES-CBC 모드로 다시 암호화하는 것은 비교 분석 대상이 되지 못한다고 여겨져 항목에 포함시키지 않았다. 보안 알고리즘에서 기본적으로 제공해야 하는 항목들에 대해 본 논문에서 제시하는 알고리즘과 기존의 연구 방법을 비교해본다.

〈표 1〉 기존의 IV 공격 방어와의 성능 비교

	IV공격 / 알고리즘	Man in the middle attack	재전송 공격	무결성	인 증
기존 IV 방어 알고리즘	IV 크기 변환 [15]	방어 불가	방어 불가	보장 불가	인증 불가
	해쉬 함수 [1]	인증 가능	탐지 가능	보장 가능	인증 가능
본 논문에서 제시하는 알고리즘	DES-ECB & 메시지 인증	방어 가능	방어 가능	보장 가능	인증 가능

• Man in the middle attack

이 공격은 공격자가 실제의 송수신 측인 것처럼 위장하여 데이터가 전송되는 중간에 끼어들어 접근하는 것을 말한다. 관련 연구에서 IV 크기 변환 방법은 단지 4, 8비트 길이의 IV를 미리 약속한 것에 따라 길이를 바꿔가며 적용시켜 전송하는 것이므로 중간에서 공격자가 위장할 확률이 크다. 따라서 Man in the middle attack에 대한 방어가 불가능하다. 여러 가지 값의 길이가 아닌 두 가지 경우에 맞춰서 데이터와 IV 값을 전송한다면 중간에서 공격당할 확률이 너무 커진다. 기존의 연구 방법 중의 또 다른 제안인 해쉬 함수를 이용한 알고리즘은 수신 측에서 같은 해쉬 함수를 적용해 값이 바뀌었는지 확인할 수 있기 때문에 인증의 기능을 수행할 수 있

다. 이 방법은 상대방에서 같은 해쉬 함수를 적용하여 인증 여부를 알 수 있다. 이 방법으로 공격에 대한 방어는 불가능하지만 데이터가 공격받은 것을 수신 측에서 감지해 낼 수 있다. 해쉬 함수 알고리즘을 적용하기 위해서는 공격을 감지 한 후에 이루어져야 하는 후의 대비책에 관한 연구도 이루어져야 한다. 본 논문에서 제안한 알고리즘은 IV 암호화와 그 값을 인증 함수를 통해 보장해주기 때문에 Man in the middle attack에 대해 안전한 방어를 제공한다.

단순히 인증 기능만 제공하는 것이 아니라, 그 전에 IV 값에 대한 암호화도 하므로 한번 더 IV 값을 보호할 수 있다.

• 재전송 공격

재전송 공격은 공격자가 중간에서 가로챈 정보를 변경하여 그 변경된 정보를 재사용하여 원래 의도되지 않은 곳으로 전송을 할 수 있고 데이터의 정보들을 공격자가 볼 수도 있는 공격 방법이다. 기존 연구 방법 중 IV 크기 변환 알고리즘은 단지 길이에 변화를 주므로 공격자가 값을 쉽게 바꿀 수 있으므로 재전송 공격을 방어할 수 없다. Man in the middle attack 공격과 비슷하게 중간에서 공격당하면 그 값을 재전송하는 것은 쉬워진다. 해쉬 함수를 이용한 알고리즘은 단지 수신 측에서 같은 해쉬 함수를 적용해 결과 값을 비교하므로 재전송 공격이 이루어진 경우에 보안 대책이 없다. 공개적으로 전송되는 IV 값을 보호하지 않기 때문에 재전송 공격을 방어하기에는 미흡한 면이 많다. 본 논문에서 제시하는 알고리즘은 중간에서 일어나는 공격을 방어하기 위해 IV 암호화와 메시지 인증 함수를 같이 적용하므로 중간의 공격자가 데이터 내용을 볼 수 없고, 수신 측에서 변경된 값을 알아챌 수 있다. 따라서 암호화와 인증을 사용하여 좀 더 안전한 IV 전송을 보장한다. 그리고 암호화를 사용하여 중간에서 공격당하더라도 다른 방법으로 재사용이 불가능하므로 재전송 공격을 방어할 수 있다.

• 무결성

무결성은 전달된 데이터가 중간에서 변경되지 않고 수신 측에 안전하게 전송되었음을 보장한다. IV 크기 변환 알고리즘은 단지 IV 값의 길이만 바꿔주므로 무결성에 관한 내용이 포함되지 않는다. 중간에서 공격자가 같은 길이의 변경된 IV 값을 이용하여 재전송 공격을 할 경우에 수신 측에서는 그걸 알아낼 방법이 없다. 해쉬 함수를 적용한 알고리즘은 수신 측에서 송신 측과 같은 해쉬 함수를 적용해서 결과 값을 비교해 무결성 여부를 확인할 수 있다. 이 알고리즘에서는 공격에 대한 방어는 할 수 없지만, 수신 측에서 공격당하고 난 다음에 재전송 알고리즘이나 복구 알고리즘을 추가해야 한다. 마지막으로 본 논문에서 제시하는 DES-ECB 암호화와 메시지 인증 함수 알고리즘은 IV 값 암호화와 메시지 인증 함수를 적용하였으므로 수신 측에서 인증 함수를 적용하여 값을 비교함으로써 무결성에 관한 내용 보장이 가능하다.

• 인증

인증은 데이터가 올바른 송신 측에게서 왔음을 보장한다. IV 크기 변환은 단순히 IV의 길이만 변화시키는 것이므로 메시지 인증 기능을 제공하지 못한다. 앞에서의 항목과 마찬가지로 중간에서 공격당할 위험도 많고, 사용자에 관한 인증 내용을 포함하지도 않는다. 인증의 기능을 제공하려면 IV 길이의 변화에 좀 더 강화된 알고리즘을 추가 적용해야 한다. 해쉬 함수를 적용한 알고리즘은 수신 측에서 같은 해쉬 함수를 적용하여 결과값을 확인해 봄으로써 인증을 보장한다. 이 경우에 해쉬 함수를 잘 결정하여 중간에서 공격자가 사용된 해쉬 함수를 알아채지 못하게 해야 한다. 본 논문에서 제시하는 알고리즘은 메시지 인증 함수를 사용하므로 안전하게 메시지 인증을 보장한다.

본 논문에서 제안한 알고리즘은 IV를 암호화하기 때문에 Man in the middle attack, 재전송 방지 및 보호 기능이 제공된다. 그리고 메시지 인증 함수를 통해 전체 ESP 데이터의 인증을 보장하는 기능을 추가했으므로 무결성 보장과 인증의 기능도 지원한다. 위에서 비교 대상으로 제시한 기존의 알고리즘에서 해쉬 함수를 적용한 경우나 IV 크기 변화 알고리즘 등 하나의 알고리즘을 적용한 경우에는 사용하는 방법에 따라 일부분의 공격에 대한 방어만 가능하다. 따라서 하나의 알고리즘을 사용하는 것보다 본 논문에서 제시하는 알고리즘처럼 IV 값도 보호하면서 메시지에 대한 인증까지 제공하는 방법이 IV 값의 안전한 전송을 보장할 수 있다.

위와 같이 본 논문에서 제시한 알고리즘은 기본적인 항목에 대해 적절한 방어 기능을 제공하고 있다. 본 논문에서 제안된 알고리즘은 공개적으로 전송되는 IV 값의 보안에 중점을 두었다. IPSec에서 기본적으로 제공하고 있는 함수와 알고리즘을 사용하여 추가적인 구현이나 오버 헤드가 발생하지 않도록 노력하였다. IV 값을 보호하기 위해 암호화 과정이 수행되고 수신 측에서 복호화 과정이 이루어지는 것은 DES 암호에서 가장 간단한 모드인 ECB 모드를 사용하여 쉽고 빠른 복호화 과정으로 큰 오버헤드가 발생하지 않는다.

5. 결론 및 향후 과제

본 논문에서 다루는 주제는 공개적으로 전송되는 IV 값에 암호화를 추가함으로써 안전한 전송을 보장하고 중간에서 일어나는 공격을 방어하고자 하는 것이다. 알고리즘은 IPSec의 ESP 프로토콜에서 일어나기 쉬운 IV 공격을 방어하기 위해 DES-ECB 모드를 이용하여 IV를 암호화한다. 이것은 공개적으로 노출되어 전송되는 IV의 값을 캡슐화 함으로써 공격자가 중간에서 IV 값에 접근할 수 없게 만든다.

본 논문에서는 IV 암호화뿐만 아니라 데이터에 대한 무결성을 추가 제공하기 위해 메시지 인증 함수를 사용한다. 함수 값은 ESP 헤더의 아랫부분인 인증 데이터 필드에 포함되어 전송된다. 메시지 인증 함수를 사용하기 위해 통신 개체는 실제 ESP 데이터를 전송하기 전에 SA의 두 번째 쿼 모드에서 메시지 인증에 관한 항목들을 결정한다. 이러한 알고리즘으로 공중

망을 통한 패킷 전송시 IV 공격에 대한 방어를 할 수 있을 뿐 아니라 전체적인 데이터의 안전을 보장하는 알고리즘이 된다.

알고리즘에 적용되는 모든 함수들과 키 값, 결정 사항들은 IPSec에서 기본적으로 제공하고 있는 것들을 사용하므로 다른 추가 설치 비용과 협상 시간이 들지 않는다. 따라서 오버헤드를 줄어들고 빠른 수행을 장점으로 가진다.

본 논문에서는 좀 더 안전하고 간단한 방법으로 안전한 IV 전송을 보장하는 알고리즘 개발을 향후 과제로 삼는다. IPSec은 공용 네트워크 망을 통해 데이터를 전송하는 것이므로 네트워크에 부하가 걸리지 않으면서 전송하기 전과 전송되어 패킷을 받은 다음 빠르게 결과 값 계산을 가능하게 하면서 중간 공격에 대한 방어와 안전한 전송을 보장하는 알고리즘 개발에 중점을 둔다. 본 논문에서 사용하는 IV 암호화 알고리즘은 암호화된 IV를 다시 복호화하기 위해 발생하는 약간의 오버 헤드를 보완하기 위해 간단한 DES-ECB 알고리즘을 사용하여 최대한 빠르고 간편하게 복호화되도록 하였고 키 값도 SA 단계에서 DES-CBC 모드에서 사용하기 위해 협상한 키 값을 그대로 사용했다. 메시지 인증 함수도 IPSec에서 구현하고 있는 함수들을 SA 단계에서 협상하여 사용함으로써 재사용성을 높였다.

앞으로 간단하고 확실한 보안을 제공하면서 ESP 헤더와 IV를 보호할 수 있는 방법에 대한 연구가 진행되어야 한다. 그리고 ESP 헤더에서의 문제점뿐 아니라 IPSec의 다른 여러 문제점들도 진단하여 해결할 수 있는 방안이 연구되어야 할 것이다.

참 고 문 헌

[1] Christopher B. MaCubbin and Ali Aydin Selcuk, "Initialization Vector Attacks on the IPSec Protocol Suite," IEEE Trans. Commun., Vol.17, No.6, June, 2000.

[2] Naganand Doraswamy and Dan Harkins, IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Prentice Hall. Networking, Vol.4, pp.885-901, Dec. 1996.

[3] S. Kent and R. Alkinson, IP Encapsulation Security Payload(ESP), Internet RFC 2406, November, 1998.

[4] Steven M. Bellovin, "Problem Areas for the IP Security Protocols," 1996.

[5] P. Karn, P. Metsger and W. Simpson, The ESP DES-CBC Transform, Internet RFC 1829, August, 1995.

[6] S. Kent and R. Atkinson, IP Authentication Header, Internet RFC 2402, November, 1998.

[7] Bruce Schneier, Applied Cryptography Second Edition, John Wiley & Son, Inc., 1996.

[8] D. Harkins, D. Carrel, The Internet Key Exchange, Internet RFC 2409, November, 1998.

[9] S. Kent and R. AtKinson. Security Architecture for the Internet Protocol, Internet RFC 2401, November, 1998.

[10] James S. Tiller, IPSec Virtual Private Networks, Auerbach Publications, 2001.

[11] William Stallings, Network Security Essentials, Prentice Hall, 2000.

[12] D. Comer. Internetworking with TCP/IP, volume 1 : Principles, Protocols, and Architecture, Prentice Hall, 1995.

[13] D. Maughan, M. Schertler, M. Schneider, Internet Security Association and Key Management Protocol (ISAKMP), Internet RFC 2408, November, 1998.

[14] http : //www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/12cmdsum/12cssec/cs_ipsec.htm# xtocid92300.

[15] C. Madson, N. Doraswamy, The ESP DES-CBC Cipher Algorithm with Explicit IV, Internet RFC 2405, November, 1998.

[16] 김창배, 박성준, 김창수, "IPSec을 이용한 가상 사설망 구현", 한국멀티미디어학회, 1999.

[17] 민병찬, "안전한 IPSec 기반 VPN 구현 방안", 동국대 국제정보대학원 석사학위 논문, 2001.

[18] 천석환, "이동 IP 에서의 보안 IPSec 프로토콜 설계", 숭실대 대학원 석사학위 논문, 1998.

[19] 안남환, "IPSec을 기반으로 한 선택적 보안 서비스를 지원하는 SG 설계 및 구현", 건국대 대학원 석사학위논문, 1999.

[20] 정미라, "가상 사설망 서비스를 위한 IP 기반 Layer Two Tunneling Protocol 구현", 숙명여대 대학원 석사학위논문, 2000.

[21] 김기현, 김홍근, "IPv6와 IPSec", 한국통신학회지, 16, 11('99.11), pp.71-86, 1999.

[22] 조인준, "인터넷 보안 메커니즘에 관한 연구", 통신정보보호학회지, 8, 2('98.6), pp.19-36, 1998.

이 영 지

e-mail : yjlee@netlab.korea.ac.kr

2000년 덕성여자 대학교 전산학과 졸업 (학사)

2000년~현재 고려대학교 컴퓨터학과 석사과정 재학

관심분야 : 인터넷 보안, 네트워크, 분산 객체

김 태 윤

e-mail : tykim@netlab.korea.ac.kr

1981년 고려대학교 산업공학과 학사

1983년 미국 Wayne State University 전산과학과 석사

1987년 미국 Auburn University 전산과학과 박사

1988년~현재 고려대학교 컴퓨터학과 교수

관심분야 : 전자상거래, 컴퓨터 네트워크, EDI, 이동통신, 멀티미디어 등