通信情報保護學會論文誌
第 7 卷 第 4 號, 1997. 12

안전한 IP 데이터그램을 이용한 정보보호 방식

박 응 기*, 손 기 욱*

Security Scheme Using Secure IP Datagram

Eungki Park, Kiwook Sohn

요 약

TCP/IPv4 정보보호를 위하여 본 논문에서는 사용자 인증, 전송 데이터의 기밀성 및 데이터의 무결성을 보장해 줄 수 있는 프로토콜 스택과 안전한 IP 데이터그램을 제안하였다. 또한 look-up 형태의 액세스 테이블을 이용해 정보보호 모듈이 있는 사용자는 물론 정보보호 모듈이 없는 사용자와도 자유롭게 정보를 교환할 수 있도록 하는 방법을 제시하였다.

Abstract

In this paper, for TCP/IPv4 security we propose a protocol stack and secure IP datagram of TCP/IPv4 protocol which provide user authentication, data confidentiality and data integrity so that some of the users of internet can communicate securely. We also propose a scheme that users may communicate each other who have the security module or not, by using a look-up access table.

I. 서 론

통신망 기술, 교환 기술, 전송 기술, 컴퓨터 기술 그리고 단말 기술의 급격한 발달은 정보통신 분야에 많은 영향을 주었고, 인터넷 발전에 크게 기여했다. 현재 인터넷에 연결된 세계 각국의 네트워크는 수 만개에 이르고 있으며, 이들 네트워크에 연결된 호스트 컴퓨터만도 수 백만 대에 이르고 있으며, 사용자도 수 천만 명에 이르고 있다[1]. 세계 각국은 인터넷의 접속을 통하여 실시간으로 각종 최신의 정보를 수집, 가공하고, 서로 정보를 교환하고 있다. 이러한 인터넷의 발달로 사용자들은 음성 및 비음성 등의 다양한 멀티미디어 정보 획득과 유통에 상당한 편익을 누리고 있는 반면에

* 한국전자통신연구원

인터넷에는 많은 해커들이 존재하고 있으며[1], 이들은 인터넷에 연결된 정부 기관, 연구소, 학교 및 회사 등의 호스트에 침입하여 시스템을 파괴하거나, 중요한 정보를 삭제 및 변형시키고[1][2][3][4], 갈취한 중요 정보를 다른 곳에 불법 이용하기도 한다. 인터넷을 통해 전송되는 정보들은 제3자에게 노출될 가능성이 훨씬 많아 졌으며, 해커와 같은 불법 침입자들의 위협은 날로 증가하고 있다[1][2][5]. 이러한 일들은 세계 각국의 도처에서 발생하고 있으며, 프로토콜 자체의 문제점을 이용[6][7][9]하거나 능동적으로 혹은 수동적으로 프로토콜을 이용하는 공격 형태[4][5][6][7][9]도 다양하다.

따라서 인터넷을 통한 정보의 유통시 전송 정보에 대한 보호 방식을 연구할 필요성이 대두되게 되었다. 인터넷을 통해 유통되는 정보를 보호하기 위해서는 인증(Authentication) 서비스, 접근제어(Access Control) 서비스, 데이터 기밀성(Data Confidentiality) 서비스, 데이터 무결성(Data Integrity) 서비스 그리고 부인 봉쇄(Non-repudiation) 서비스 등이 필요하다[2].

본 논문에서는 어떠한 인증 알고리듬과 정보보호 알고리듬의 사용에 관계없이 그리고 상위 계층에서 사용되는 프로토콜에 상관없이 TCP/IPv4 (Transmission Control Protocol / Internet Protocol version 4) 프로토콜을 이용해 정보가 유통될 때 유통되는 정보를 보호하는 방법을 제시한다. 본 논문에서 제시한 네트워크 정보보호 방법과 방화벽 시스템[3]을 이용하면 인터넷에 연결된 네트워크(회사의 사설 네트워크, 정부의 행정망, 연구망, 국방망, 금융망 등)를 외부의 네트워크에 존재하는 해커 및 불법 침입자들로부터 보다 안전하게 보호할 수 있다.

본 논문의 구성은 II장에서 TCP/IPv4 프로토콜에 대한 개념 파악 및 프로토콜의 구조를 분석하고, III장에서는 프로토콜 구조에 입각한 TCP/IPv4 네트워크의 정보보호 방법을 제시하며, 마지막으로 IV장에서 결론을 맺는다.

II. TCP/IP 프로토콜[8]

TCP/IP 프로토콜은 컴퓨터들 간에 네트워크를 통해 자원들을 공유할 수 있도록 하기 위해 미국 국방성의 지원 하에 개발되어 ARPANET에 사용되었으며, 이후로 대부분의 네트워크에서 이를 수용하였으며, 현재 인터넷에서 사용되고 있다. TCP/IP 프로토콜은 OSI(Open System Interconnection) 참조 모델의 계층 4에 해당하는 TCP 프로토콜과 계층 3에 해당하는 IP 프로토콜로 구성되어 있다. 이들 TCP/IP 프로토콜은 FTP(File Transfer Protocol), TELNET, SMTP(Simple Mail Transfer Protocol), RPC(Remote Procedure Call) 등과 같은 서비스를 지원해 준다. 본 장에서는 TCP/IP 프로토콜의 개념과 구조에 대해 분석한다.

1. 프로토콜

1.1 TCP 프로토콜

TCP는 응용에 대해 신뢰성 있는 데이터 전송 서비스를 제공하는데, 이를 위해 TCP에서는 에러가 없는 완벽한 데이터의 전송 기능 및 송신 측에서 보낸 순서대로 수신할 수 있는 제어 기능을 갖는다. TCP는 응용 계층의 사용자 정보를 세그먼트 단위로 나누어 IP 계층으로 전달하여 목적지까지 전송되도록 한다. 수신 측의 TCP는 IP로부터 세그먼트를 수신하여 송신된 순서대로 정보를 가공하여 응용 계층에 제공한다.

1.2 IP 프로토콜

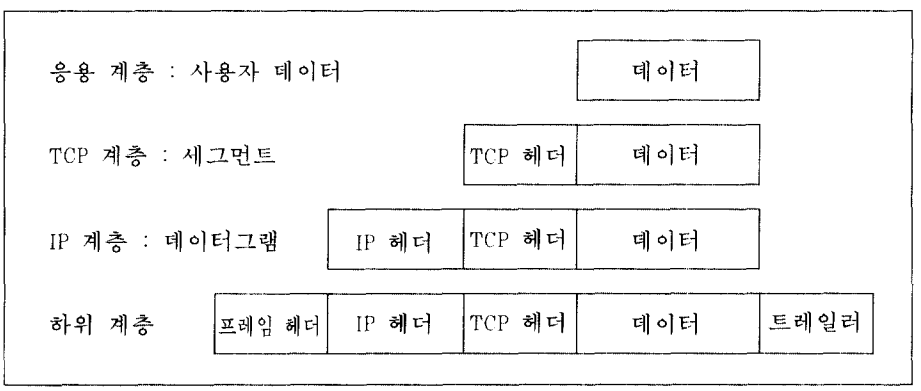
IP는 네트워크에 연결된 호스트 컴퓨터 사이의 라우팅을 제어하여 정보를 교환할 수 있도록 한다. IP에서의 데이터 처리 단위는 데이터그램(Datagram)이며, TCP 계층에 정보 전달을 위한 서비스를 제공하는 무연결 지향(Connectionless Oriented) 프로토콜이다. 전달되는 데이터그램은 독립적으로 라우팅되어 전달되기 때문에 IP계층에서는 전송정보의 순서를 유지하거나 신뢰성을 보증할 수 없다.

2. 응용 서비스

TCP/IP 프로토콜은 프로그램 대 프로그램 통신 등의 많은 응용 서비스를 지원하고 있다. 이러한 응용 서비스는 FTP, SMTP, TELNET, DNS(Domain Name System), NFS(Network File System) 등이 있다.

3. 프로토콜 데이터 단위

TCP/IP 프로토콜 구조는 상위 계층에는 응용 계층만을 두고 있으며, 하위 계층에는 계층 2와 계층 1로 구성되어 있다. 응용 계층의 응용들은 상대방과 정보를 교환하기 위하여 TCP 계층과 IP 계층 그리고 하위 계층의 서비스를 이용하며, 각 계층에서 처리되는 데이터의 단위는 각각 다르게 존재하며, 이들의 구성은 [그림 1]과 같다.



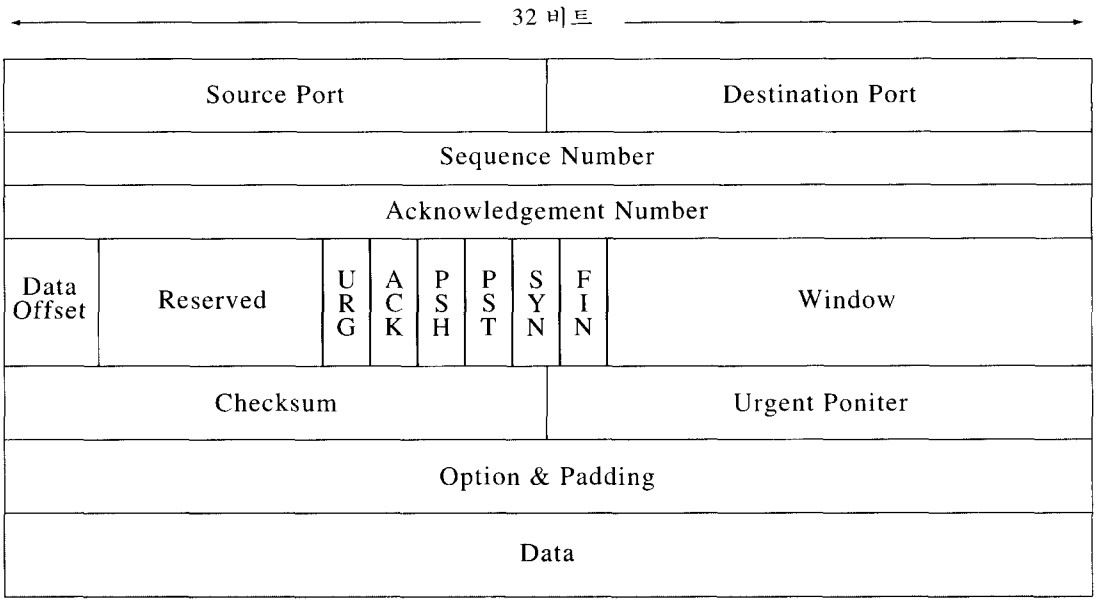
[그림 1] 프로토콜 데이터 단위

3.1 TCP 세그먼트 형식

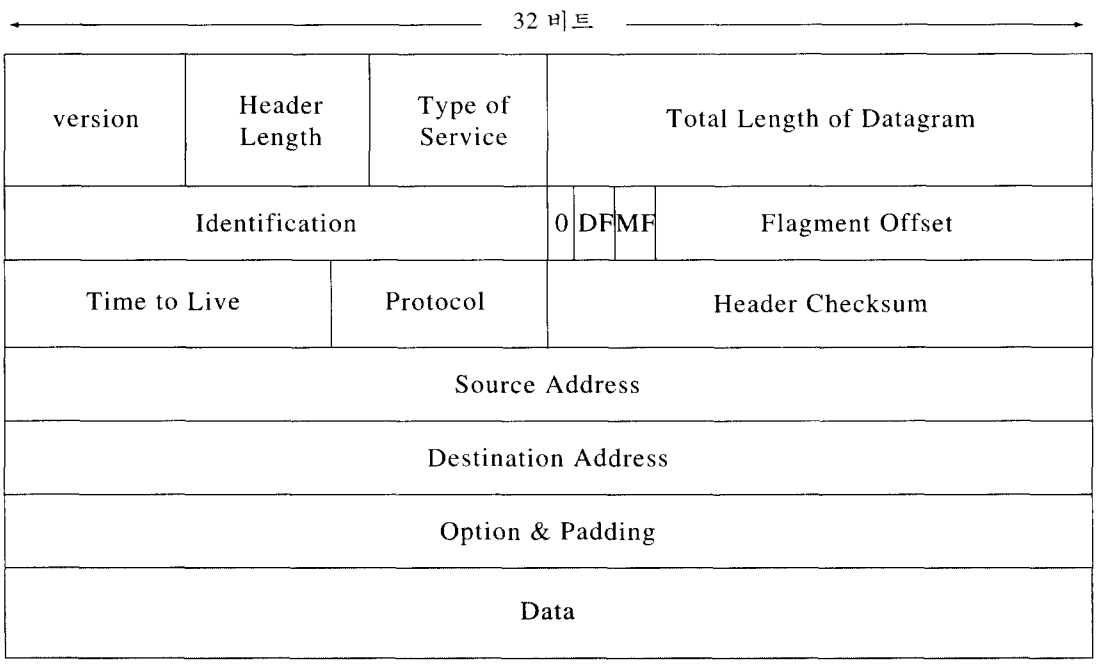
TCP는 정보의 전송을 위해 우선 연결(Connection)을 설정하고, 정보를 전송하며, 연결을 단절시키는 연결 지향(Connection Oriented)적인 프로토콜이다. TCP의 세그먼트는 [그림 2]와 같은 형식으로 구성되어 있다.

3.2 IP 데이터그램 형식

본 논문에서는 IP 프로토콜의 버전 4를 대상으로 설명하고자 한다. IP 데이터그램의 헤더는 최대 60바이트로 구성되며, 보통은 최소 단위인 20바이트를 사용하고 있다. IP 데이터그램의 형식은 [그림 3]과 같다. Destination Address의 다음 필드에 존재하는 Options 필드는 데이터그램 및



[그림 2] TCP 세그먼트 형식



[그림 3] IP 데이터그램 형식

네트워크 제어 그리고 네트워크의 디버깅 등을 위해 사용되고 있다. 이러한 Option 기능은 선택 코드 바이트로 정의되어 있다. 따라서 특정 Option을 사용하기 위해서는 사용하고자 하는 Option에 해당하는 선택 코드 바이트를 Options 필드에 나타

내야 하며, 선택 코드 바이트의 다음 필드부터 실행하고자 하는 내용을 나타내면 된다. 선택 코드 바이트의 형식은 [그림 4]와 같다.

Copy(1Bit)	Option Class (2Bits)	Option Number(5bits)

[그림 4] 선택 코드 바이트

III. TCP/IP 네트워크 정보보호

1. 정보보호 대상

TCP/IP 기반의 네트워크에서의 정보보호 대상은 TCP와 IP의 헤더에 있는 모든 제어 정보 및 사용자 데이터를 보호하는 방법과 응용계층의 순수 사용자 데이터만을 보호하는 방법으로 나눌 수 있다.

1.1 모든 데이터의 보호

이 방법은 응용 계층에서 전송하고자 하는 사용자 데이터 및 TCP 계층과 IP 계층에서 사용되는 제어 정보 모두를 보호하는 방법이다. 이 방법은 TCP/IP에서 사용되는 프로토콜 및 제반 제어를 모르더라도 쉽고 간단하게 실현할 수 있으나, 프로토콜 자체도 보호함으로써 프로토콜 투명성이 상실되어 사용자 정보의 전송을 위한 라우팅을 할 수 없으며 이로 인해 프로토콜을 인식하는 중간의 모든 노드마다 정보보호 모듈이 존재하여야만 한다. 따라서 이 방법을 사용하기 위해서는 점 대 점(point-to-point) 방식의 정보보호 방식을 사용하여야 하나, 인터넷에 적용하는 것은 현실성이 없다.

1.2 사용자 데이터의 보호

이 방법은 응용 계층에서 전송하고자 하는 사용자의 데이터만을 보호하는 방법이다. 사용자의 유통 정보만을 보호하기 위해서는 TCP/IP에서 사용하는 모든 프로토콜 및 제반 사항을 알아야 가능하기 때문에 실현하기 어렵고 시간이 많이 든다. 그러나 TCP/IP에서 사용하는 프로토콜 자체는 보호하지 않기 때문에 프로토콜 투명성을 잘 유지할 수 있으며, 또한 이 방법은 통신망과는 투명하게 처리되므로 네트워크를 구성하는 중간 노드들과 관계없이 단 대 단(end-to-end) 방식의 정보보호 방식을 실현할 수 있다.

따라서 프로토콜 투명성을 유지하면서 정보보호 서비스를 실현할 수 있는 사용자 데이터만을 보호하는 것이 타당하리라 판단된다.

2. 정보보호 방법

본 논문에서는 네트워크에 대해 투명성을 유지하면서 사용자의 데이터를 보호하는 단 대 단 방식의 정보보호 방식을 사용한다. 따라서 중간 노드들은 사용자의 데이터가 어떠한 가공이 되어 전송되는지 알 필요가 없으며, 네트워크 상에서 전송되는 데이터를 제3자 및 중간 노드 그리고 전송로로부터 보호할 수 있다. 이러한 방식은 현재 네트워크의 하부 구조 및 인터페이스 등의 변경 없이 적용 가능하다. 본 논문에서 제공하는 정보보호 서비스는 다음과 같다.

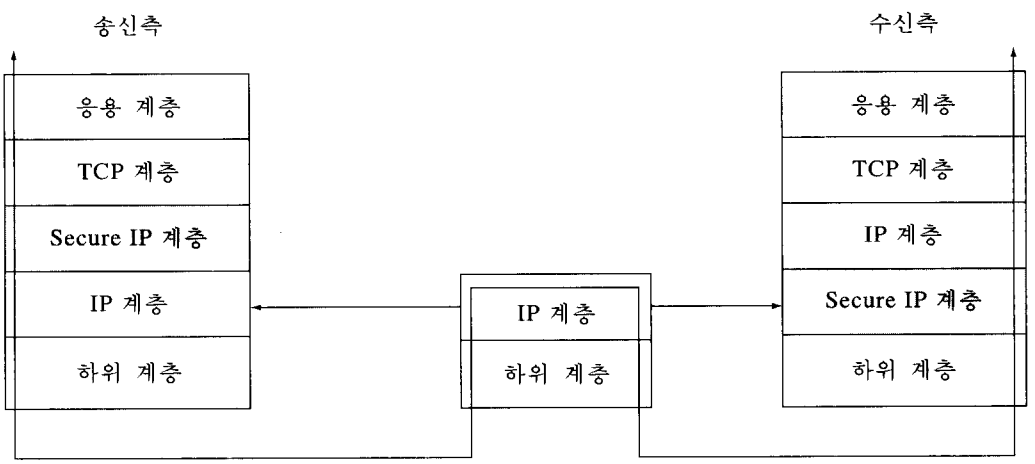
- 데이터 기밀성 (Confidentiality) : 전송되는 데이터에 대한 제3자로부터 보호 기능

- 데이터 무결성(Integrity) : 전송 데이터의 삽입, 삭제 및 변경 등에 대한 보호 기능
- 인증(Authentication) : 단 대 단의 통신 당사자들을 인증하여 불법 침입자를 방지

인터넷을 사용하여 정보를 교환할 경우는 상대방이 정보보호 모듈이 없을 경우도 정보 교환이 가능해야 한다. 정보의 바다라고 불리는 인터넷에 산재해 있는 다양한 정보를 접하기 위해서는 상대방이 정보보호 모듈을 가지고 있든 혹은 없든 간에 상호 통신이 가능하게 하는 것도 정보보호의 실현만큼이나 현실적으로 중요하다. 본 논문에서는 이러한 사항을 만족할 수 있도록 정보보호 모듈의 존재 여부를 IP 주소와 같이 관리하여 이를 해결하는 방법을 제시한다.

2.1 정보보호 프로토콜 스택

정보보호 프로토콜의 중요한 기능은 전송 데이터의 기밀성을 유지하면서 데이터의 안전한 전송에 있으며, 더불어 전송 데이터에 대한 무결성을 유지할 수 있어야 한다[12]. 이를 위해서 본 논문에서는 안전한 정보 전송을 위해 [그림 5]와 같은 프로토콜 구조를 갖도록 설계하여 단 대 단의 정보보호를 실현하며, 단 대 단의 정보를 안전하게 전송하기 위해 [그림 5]에서 보는 바와 같이 기존 TCP/IP 프로토콜 구조에서 계층 3인 IP 계층에 Secure IP 부 계층을 삽입한 구조로 프로토콜 스택을 설계한다. Secure IP 부 계층의 기능은 사용자 데이터의 기밀성을 유지하도록 암호화/복호화 기능을 수행하고, 통신을 원하는 적합한 사용자인지를 결정하기 위한 인증 기능을 수행하며 전송 데이터에 대한 무결성을 보장할 수 있도록 한다. 이러한 정보보호 서비스를 제공하기 위해 사용되는 알고리듬은 어떠한 것이라도 관계없다. 예를 들어 전송 데이터의 암호화 및 복호화를 수행하기 위한 알고리듬은 DES, Triple DES 혹은 IDEA[12] 등을 사용하여도 무관하며, 전송 데이터의 무결성 점검을 위해 MD4 혹은 MD5[12] 등을 사용하며, 인증을 수행하는 알고리듬은 Kerberos[12] 등을 사용할 수 있다.



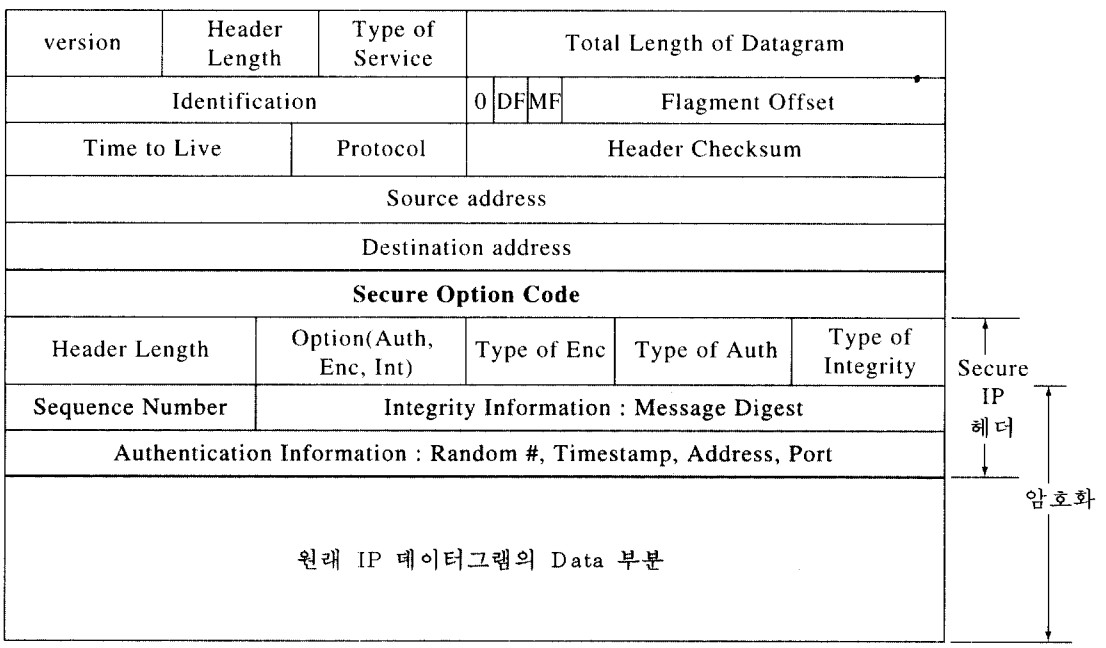
[그림 5] 제안한 프로토콜 스택

2.2 안전한 IP 데이터그램 형식

TCP/IP 프로토콜을 사용하는 네트워크에서 전송되는 데이터의 기밀성을 유지하고, 전송 데이터의 무결성을 보장하며 인증을 수행하기 위한 IP 데이터그램의 형식은 [그림 6]과 같다. [그림 3]의 IP 데이터그램 형식에서 Option 필드에 나타나는 선택 코드 바이트의 Option Number에 본 논문에서 제공하고자 하는 기능을 나타내는 Secure Option Code를 새로이 추가 정의한다. Secure Option Code는 [그림 4]의 선택 코드 바이트 형식에서 Option Class 필드를 0으로, Option Number 필드를 F로 정의한다. Secure Option Code가 IP 데이터그램의 Options 필드에 존재하면 이후의 정보는 본 논문에서 제시하는 Secure IP 헤더로 인식하며, Secure IP 헤더의 내용에 따라 TCP 세그먼트를 처리한다. 본 논문에서 제시한 방법은 단대 단의 사용자 인증 기능, 전송 데이터에 대한 무결성 점검 기능 및 전송 데이터의 기밀성 유지를 위한 암호화/복호화 기능은 선택적으로 사용 가능하다. 이러한 기능을 선택적으로 사용하는 목적은 정보보호 모듈이 존재하지 않는 상대방과도 정보를 자유롭게 교환할 수 있도록 하기 위함이다. [그림 6]에서 Secure IP 헤더와 원래 IP 데이터그램의 Data 부분은 IP 데이터그램이 전송도중 네트워크 상에서 제3자에게 노출되지 않도록 하기 위해 암호화할 수 있다. 암호 알고리듬은 여러 가지가 사용될 수 있으며, 사용되는 알고리듬은 Secure IP 헤더에 표시할 수 있도록 하였다.

Secure IP 헤더를 구성하는 각 필드의 구성 및 내용은 다음과 같다.

- Header Length : Secure IP 헤더의 길이를 바이트 단위로 표시한다. 이 필드는 2 바이트의 길이를 갖는다.
- Option(Auth, Enc, Int) : Secure IP 헤더 내



[그림 6] 안전한 IP 데이터그램 형식

에 인증 정보를 포함시킬 것인지, IP 데이터그램의 Data 부분을 암호화할 것인지, 그리고 전송되는 정보에 대한 무결성 점검을 수행할 것인지를 결정하는 필드이다. 수신 측은 이 필드에 따라 인증 수행 여부 결정, IP 데이터그램의 Data 부분을 복호화할 것인지, 그리고 IP 데이터그램의 Data 부분에 대한 무결성 점검 기능을 수행할 것인지를 결정하여 수행한다. 이 필드는 1 바이트의 길이를 갖는다.

- Type of Enc : Secure IP 헤더 부분(Sequence Number 부터 Authentication Information 까지)과 원래 IP 데이터그램의 Data 부분을 암호화/복호화하는데 사용하는 암호 알고리듬을 나타낸다. 이 필드는 1 바이트의 길이를 갖는다.
- Type of Auth : 인증 정보에 의한 단 대 단 인증에 사용될 인증 알고리듬을 나타낸다. 이 필드는 1 바이트의 길이를 갖는다.
- Type of Integrity : Secure IP 헤더와 원래 IP 데이터그램의 Data 부분에 대한 데이터 무결성을 유지하기 위해 사용되는 알고리듬을 나타낸다. 이 필드는 1 바이트의 길이를 갖는다.
- Sequence Number : Secure IP 데이터그램의 순서 번호를 나타내며, 이는 공격자에 의한 Replay 공격에 대비하기 위해 인증 정보에 포함된 내용과 함께 이용된다. 이 필드는 1 바이트의 길이를 갖는다.
- Integrity Information : 이 필드 이후부터의 정보에 대한 무결성 정보를 전달하는 필드이다. 무결성 정보는 사용되는 무결성 유지를 위한 알고리듬에 따라 달라질 수 있다. 이 필드는 최대 30 바이트의 길이를 갖는다.
- Authentication Information : 사용자 인증을 위해 여러 가지 정보를 이용하는데, TCP 연결을 설정하는 과정에서는 Random Number, Timestamp, 근원지 및 목적지의 IP 주소와 포트 번호를 이용하여 인증을 수행하며, TCP 연결이 설정된 후 데이터 전달 단계에서는 위의 정보 중 Random Number 를 뺀 나머지 정보를 가지고 매 IP 데이터그램마다 인증을 수행하도록 한다. 이 필드는 최대 270 바이트의 길이를 갖는다.

3. 액세스 테이블

액세스 테이블은 근원지 주소, 근원지의 포트 번호, 목적지 주소, 목적지의 포트 주소, 프로토콜 종류 및 프로토콜 플래그, 행위(허가/거절) 그리고 정보보호 모듈의 존재 여부를 나타내는 부분으로 [그림 7]과 같이 구성된다. IP 프로토콜을 사용하는 네트워크에서 정보 교환을 위한 연결에 대한 요청이 입력되면 정보보호 모듈은 프로토콜의 헤더를 분석하여 근원지/목적지의 주소 및 포트 번호, 사용 프로토콜의 종류 및 프로토콜의 제어 필드의 내용을 분석하고, 이들을 액세스 테이블의 행위 필드를 참조하여 진입을 허용할 것인지 아니면 거절할 것인지를 판별한다. 액세스 테이블의 행위 필드를 이용하여 인터넷에 존재하는 해커들이 로컬 네트워크에 연결된 자신의 컴퓨터로 침입하는 것을 방지할 수 있다. 일단 액세스 테이블 참조에 의해 진입이 허용이 결정되면 액세스 테이블에서 상대방이 정보보호 모듈을 가지고 있는가를 판별하여, 정보보호 모듈이 존재할 경우 본 논문에서 제공하는 정보보호 서비스를 이용하여 안전한 정보 교환을 할 수 있도록 하며, 상대방에 정보보호 모듈이 없을 경우는 정보보호 서비스를 제공하지 않고 일반적인 IP 프로토콜을 이용한 정보 교환을 할 수 있도록 한다. 역으로 상대방으로 정보를 전송하는 경우도 상기와 같은 절차를 수행한다. 이렇게 함으로써 인터넷에 인가되지 않은 해커 등과 같은 불법 침입자로부터 자신의 컴퓨터를 보호할 수 있으며, 네트워크상의

제한된 사용자 혹은 모든 사용자들과 정보를 교환할 수 있으며, 중요한 정보의 교환이 일어날 경우는 통신 당사자들끼리 정보보호 모듈을 가지고 안전한 정보 교환을 할 수 있도록 한다.

규칙 번호	행위	근원지 주소	근원지 포트	목적지 주소	목적지 포트	프로토콜 플래그	정보보호 모듈 존재 여부
1	허가	129.244.1.24	1024	129.244.1.1	25	TCP	존재
2	거절	129.244.0.0	0	129.244.2.1	25	TCP	없음
..							

[그림 7] 액세스 테이블

4. 정보보호 처리 절차

본 논문에서 제안한 방법의 정보보호 처리 절차는 다음과 같다.

4.1 송신측 처리 절차

단계 1
TCP와 IP 헤더 분석

단계 2
액세스 테이블을 참조하여 평문 통신 여부 결정
평문 통신이면 IP 데이터그램을 그대로 하위 계층으로 전송하고, 암호 통신이면 단계 3을 실행

단계 3
인증 실행 여부 결정
인증 기능이 필요하면 단계 4를 실행하고, 인증 기능이 필요 없으면 단계 5를 실행

단계 4
인증 알고리듬 선택
인증 정보 구성
인증 알고리듬 구동

단계 5
무결성 실행 여부 결정
무결성 점검 기능이 필요하면 단계 6을 실행하고, 무결성 점검 기능이 필요 없으면 단계 7을 실행

단계 6
무결성 점검 알고리듬 선택
무결성 점검 알고리듬 구동
암호 알고리듬 선택
Secure IP 헤더 구성
Secure IP 헤더 암호화

단계 7
암호화 실행 여부 결정
암호화 기능이 필요하면 단계 8을 실행하고, 암호화 기능이 필요 없으면 단계 9를 실행

단계 8
암호 알고리듬 선택
TCP 세그먼트 암호화 실행

단계 9
Secure IP 데이터그램 구성
Secure IP 데이터그램을 하위 계층으로 전달
데이터 전송동안 단계 1 ~ 단계 9를 반복적으로 실행

4.2 수신측 처리 절차

단계 1
IP 헤더 분석

단계 2
액세스 테이블을 참조하여 평문 통신 여부 결정
평문 통신이면 IP 데이터그램을 그대로 상위 계층으로 전달하고, 암호 통신이면 단계 3을 실행

단계 3
Secure IP 헤더 분석
복호화 실행 여부 결정
복호화 기능이 필요하면 단계 4를 실행하고, 복호화 기능이 필요 없으면 단계 5를 실행

단계 4
암호 알고리듬 선택
TCP 세그먼트 복호화

단계 5
Secure IP 헤더 복호화

단계 6
무결성 점검 여부 결정
무결성 점검 기능이 필요하면 단계 7을 실행하고, 무결성 점검 기능이 필요 없으면 단계 9를 실행

단계 7
무결성 알고리듬 선택
무결성 알고리듬 구동 및 무결성 값 계산
무결성 점검 값 비교
무결성 점검 값이 같으면 단계 9를 실행하고, 무결성 점검 값이 틀리면 단계 8을 실행

단계 8
재 전송 요구
단계 1을 실행

단계 9
인증 기능 여부 결정
인증 기능이 필요하면 단계 10을 실행하고, 인증 기능이 필요 없으면 단계 11을 실행

단계 10
인증 알고리듬 선택
인증 알고리듬 구동 및 인증 점검
인증이 되면 단계 11을 실행하고, 인증이 안되면 단계 12를 실행

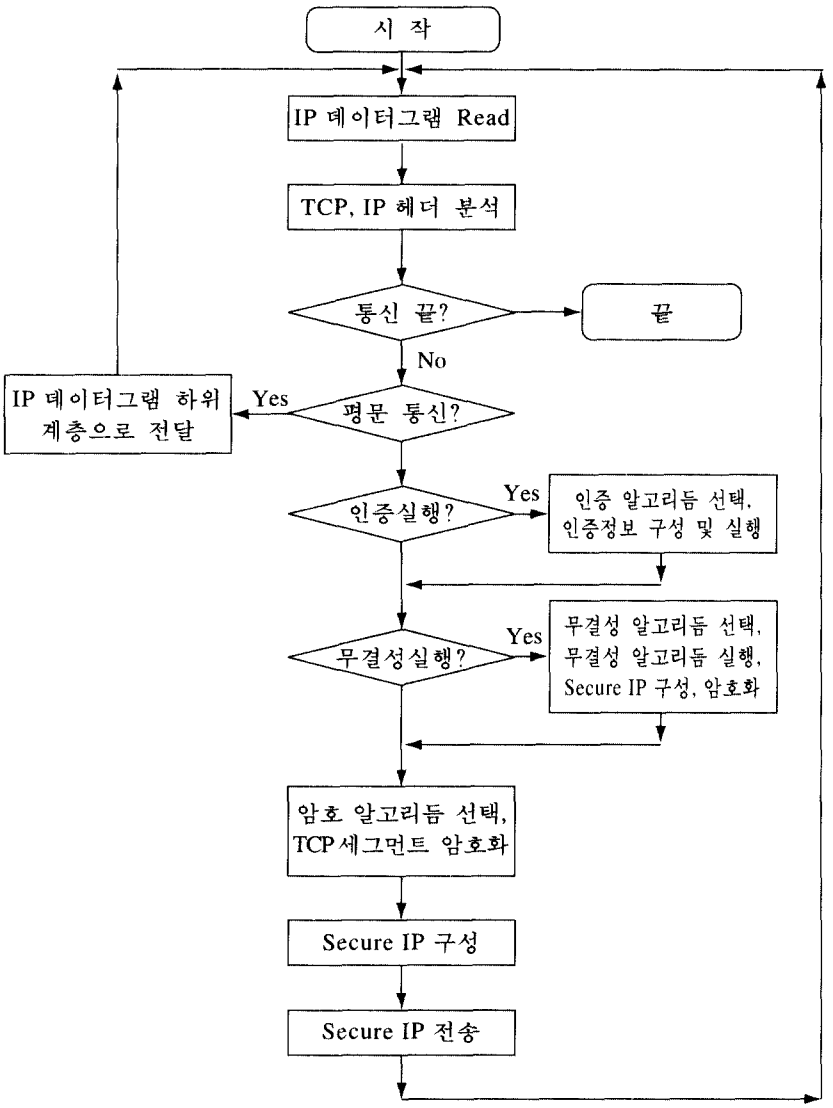
단계 11
Secure IP 헤더를 삭제하고 필요 부분만 따로 저장
제어를 상위 계층으로 넘김
데이터 전송 동안 단계 1 ~ 단계 11을 계속 실행

단계 12
통신 단절시킴

IV. 결 론

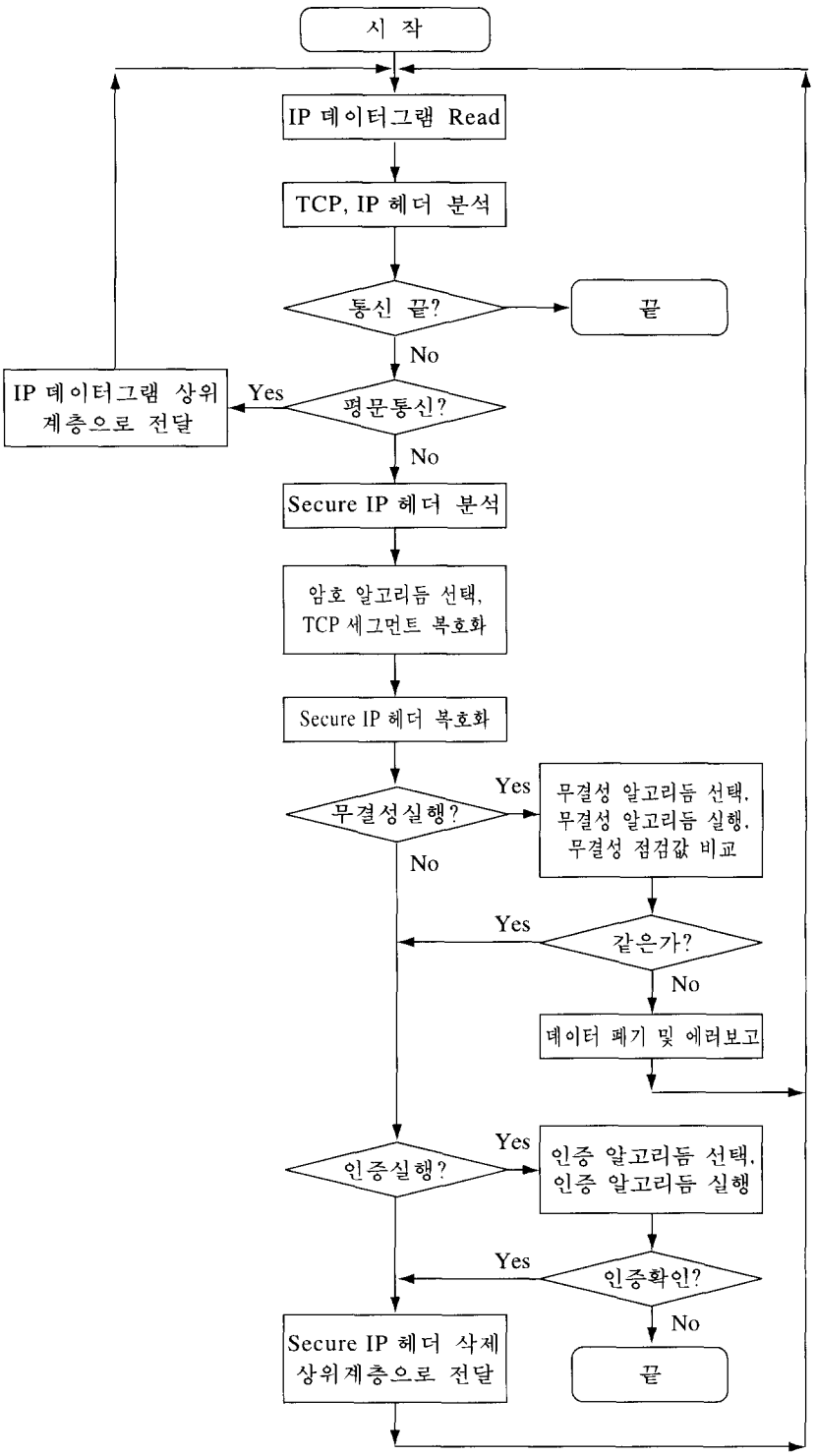
본 논문에서는 인터넷에서 사용중인 TCP/IP 프로토콜을 분석하였고, TCP/IP 프로토콜을 이용하여 네트워크를 통해 다양한 정보가 교환될 때 교환 정보의 보호 대상을 제시하였으며, 액세스 테이블을 이용하여 정보보호 모듈의 소유와 관계없이 인터넷 사용자들간에 자유롭게 정보를 교환할 수 있도록 하는 방법을 제시하였다. 또한 정보보호 모듈을 소유한 인터넷 사용자들간에는 전송 데이터의 기밀성 유지, 전송 데이터의 무결성 점검 그리고 단 대 단의 사용자 인증을 수행할 수 있도록 TCP/IP 프로토콜 구조와 안전한 IP 데이터그램 형식을 제시하였다.

향후 본 논문에서 제시한 방법을 기초로 하여 인터넷을 통한 정보 교환에 적합한 키 분배 방식 및 인증 방식 등에 대한 연구를 보다 심도 있게 하여 인터넷에 적용하면 정보를 안



[그림 8] 송신측 흐름도

전하게 전송할 수 있으며, 정보 전송에 따른
각종 분쟁을 해결할 수 있으리라 판단된다.


시 작
IP 데이터그램 Read
TCP, IP 헤더 분석
통신 끝?
끝
No
IP 데이터그램 상위 계층으로 전달
Yes
평문통신?
No
Secure IP 헤더 분석
암호 알고리듬 선택, TCP 세그먼트 복호화
Secure IP 헤더 복호화
무결성실행?
Yes
무결성 알고리듬 선택, 무결성 알고리듬 실행, 무결성 점검값 비교
No
Yes
같은가?
No
데이터 폐기 및 에러보고
인증실행?
Yes
인증 알고리듬 선택, 인증 알고리듬 실행
Yes
인증확인?
No
Secure IP 헤더 삭제 상위계층으로 전달
끝

[그림 9] 수신측 흐름도

[참 고 문 헌]

[1] K. Siyan and C. Hare, Internet Firewalls and Network Security, Indianapolis, IN:New Riders Publishing, 1995.

[2] W. Stalling, Network and Internetwork Security : Principles and Practice, Englewood Cliffs, NJ:Prentice-Hall, 1995.

[3] 박응기, 손기욱, 정현철, 전산망 보호를 위한 방화벽 시스템 고찰, 통신정보보호학회지, 제6권, 제2호, pp.5-20, 1996.

[4] CERT Advisory 95:01, IP Spoofing Attacks and Hijacked Terminal Connections, CERT Coordination Center, January 1995. Available at ftp://info.cert.org/pub/cert-advisories/CA-95:01.IP.spoofing.attack.and.hijacked.terminal.connection.

[5] L. Joncheray, A Simple Active Attack Against TCP, April 1995. Available at http://www.deter.com/unix/tcp_attack.ps.

[6] S.M. Bellovin, Security Problems in the TCP/IP Protocol Suite, Computer Communications Review, Vol. 19, No. 2, pp.32-48, April 1989. Available at http://www.raptor.com/library/ ipext.ps.

[7] S.M. Bellovin, There Be Dragons, In proc. of the Third Usenix UNIX Security Symposium, pp. 1-16, September 1992. Available at http://www.raptor.com/library/dragon.ps.

[8] Sidnie Feit, TCP/IP Architecture, protocols, and Implementation, New York, NY:McGraw-Hill, 1993.

[9] F.L. McNulty, Security in the Internet, March 1994. Available at http://www.raptor. com.library/i_netsec.txt.

□ 著者紹介

박 응 기

1986년 2월 중앙대학교 전자계산학과 이학사
1988년 2월 중앙대학교 전자계산학과 이학석사
1988년 2월 ~ 현재 한국전자통신연구원 선임연구원

※ 주관심 분야 : 통신 및 네트워크 보안, 컴퓨터 보안, 안전한 통신프로토콜

손 기 욱

1990년 2월 성균관대학교 정보공학과 공학사
1992년 2월 성균관대학교 정보공학과 공학석사
1992년 1월 ~ 현재 한국전자통신연구원 연구원

※ 주관심 분야 : 통신망 정보보호, 암호프로토콜, FPGA 설계