論文 95-9-9-18

인터네트워크에서 전송 데이타의 보호 서비스 제공 방안

正會員 朴 暎 昊*, 文 相 在*

The Providing Scheme of the Security Service for Transmitting Data in the Internetwork

Young Ho Park*, Sang Jae Moon* Regular Members

要 約

본 논문에서는 인터네트워크에서 보호를 제공하기 위한 새로운 보호영역 모델을 제안한다. 본 모델은 인터네트워크의 중간 시스템에서 인증 및 무결성 서비스를 제공하며 비밀보장 서비스는 제공하지 않는다. 따라서, 본 모델은 인터네트워크의 중간 시스템에서 전송 데이타의 인증 및 무결성을 알 수 있으며 구현이 간단하고 안전하다. 또한, 본 논문에서는 인터네트워크상에서 단편화 및 무결성 서비스를 효율적으로 제공할 수 있는 키 종속 해쉬 프로토콜을 제시하며 D-H형 키 분배 프로토콜을 이용하여 제안한 인터네트워크 보호모델에 적합한 키 분배 프로토콜을 제안한다. 제안한 키 분배 프로토콜은 DES, MD5 그리고 Montgomery 알고리듬을 이용하여 소프트웨어적으로 구현한다.

ABSTRACT

This paper presents a new protection boundary model for internetwork security. Intermediate system of our model does not fulfill security service of confidentiality but authentication and integrity. Thus this model knows whether the transmission data on the intermediate system is authentic and integral or not, and it is practical and easy to be implemented. This paper also propose a key-dependent hash protocol which can provide integrity and fragmentation efficiently, and a key-distribution protocol, which is suitable for the proposed model, using D-H type protocol. This key-distribution protocol is implemented using DES, MD5, and Montgomenry algorithm.

* 경북대학교 전자공학과
Dept. of Electronics Eng., Kyungpook National Univ.
論文番號 : 95157-0424
接受日字 : 1995年 4月 24日

Ⅰ. 서 론

인터네트워크는 다른 네트워크의 자원을 공유하거나 정보교환을 위하여 국가별,지역별 그리고 기업별로 서로 다른 특징을 갖는 여러종류의 네트워크들을 연결한다[1]. 이러한 인터네트워크에서는 중요한 정보자원에 대한 정보보호 취약성이 증가하여 중요 정보의 노출, 오용, 불법변경 그리고 파괴 등의 위협을 가지게 되어 이에대한 정보보호 체계가 절실히 요구된다. 그러나 인터네트워크에 관한 통신 기술과 병행하여 정보보호 체계 개발이 진행되지 않았다. 이러한 인터네트워크의 취약성을 대비하기 위하여 정보보호 체계의 구조 및 프로토콜 개발이 중요한 과제이다.

인터네트워크에서 안전한 통신을 위한 보호 프로토콜로는 IP(internet protocol)에서의 보호 및 OSI 구조에 기초한 보호 프로토콜(2,3)이 있다. IP는 최근 표준화를 위한 초안(IPv6, internet protocol version 6)[4,5]이 발표된 바 있다. 이 초안에서는 데이타를 보호하기 위하여 선택영역을 이용하고 있으나 구체적인 표준안은 없는 실정이다. OSI 구조에 기초한 인터네트워크 보호 프로토콜은 네트워크 계층 레벨에서 보호가 이루어지고 있으며 NIST의 SP3(security protocol 3)[6]과 ISO/IEC의 표준안인 NLSP(network layer security protocol)[3]가 있다. 이러한 보호 프로토콜들에서는 인터네트워크에서 보호서비스를 제공하기 위하여 종단 시스템에서만 보호서비스를 설정하는 방식과 종단 및 중간 시스템에 동일한 보호서비스를 설정하는 방식이 있으나 인터네트 환경을 고려한 보다 효율적인 보호체계가 요구된다.

인터네트워크에서 제공되는 대표적인 보호서비스로는 인증, 무결성, 비밀보장 그리고 접근 제어 서비스가 있다. 특히, 무결성 서비스는 인터네트워크 상에서 발생하는 단편화(fragmentation) 과정을 수용할 수 있어야 하며 무결성 서비스를 제공하는 대표적인 프로토콜로는 DA(delayed authentication) 프로토콜[7]이 있으며 MTU(maximun transmission unit) 방식(8)을 이용한 프로토콜 및 키 종속 해쉬 함수를 이용한 프로토콜도 가능하다.

본 논문에서는 인터네트워크에서 보호서비스를 제공하기 위하여 종단 시스템간에는 비밀성이 유지되며 종단 시스템과 중간 시스템간 그리고 중간 시스템들 간에 인증 및 무결성이 제공될 수 있는 보호영역 모델을 제안한다. 본 모델은 인터네트워크의 중간 시스템에서 단편화 과정을 효율적으로 처리할 수 있으며 비밀보장 서비스가 제공되지 않으므로 구현이 비교적 간단하고 안전하다. 또한, 본 논문에서는 인터네트워크상에서 무결성 서비스를 효율적으로 제공하는 키 종속 해쉬 프로토콜을 제시하며 D-H형[9,10] 키 분배 프로토콜을 이용하여 제안한 인터네트워크 보호모델에 적합한 키 분배 프로토콜을 제안한다.

Ⅱ. 인터네트워크 보호영역 모델

서로다른 특징을 갖는 여러종류의 네트워크를 연결하여 자원을 공유하거나 정보교환을 위하여 네트워크의 상호연결이 요구되었으며 미 국방성 ARPANET 프로젝트에 의해 인터네트워크에 관한 연구가 시작 되었다.[11] 인터네트워크에서의 대표적인 통신방식은 미 국방성의

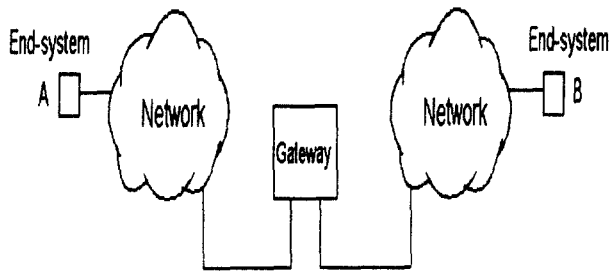


그림 1. 전형적인 인터네트워크 구성
Fig. 1. A typical topology of internetwork.

TCP/IP 프로토콜과 ISO에서 OSI 구조에 기초하여 제시한 인터네트워크 프로토콜이 있다. 그림 1은 전형적인 인터네트워크 구성(topology)을 나타낸 것이다.

인터네트워크에서 안전한 통신을 위한 보호 프로토콜로는 IP 보호 프로토콜 및 OSI 구조에 기초한 보호 프로토콜이 있다. 인터네트 프로토콜은 최근 표준화를 위한 초안이 발표된 바 있으며 선택영역을 이용하여 보호를 제공하고 있으나 구체적인 표준안은 없는 실정이다. OSI 구조에 기초한 인터네트워크 보호 프로토콜은 네트워크 계층 레벨에서 보호가 이루어지고 있으며 NIST의 SP3과 ISO/IEC의 표준안인 NLSP가 있다.

NLSP와 SP3은 비밀보장, 무결성 그리고 인증 서비스를 제공하며 보호영역은 그림 2와 같다. 그림 2(a)는 신뢰할 수 없는 중간(intermediate) 시스템으로 접속된 경우의 인터네트워크 보호영역을 나타낸 것이다. 이 경우는 네트워크 제공자 및 침입자(intruder)로부터 종단 시스템을 보호하는 방식이다. 중간 시스템에서 보호서비스가 제공되지 않으므로 구현은 비교적 간단하나 네트워크 상에서 전송 데이타의 인증 및 무결성 여부를 알 수 없는 단점이 있다. 그림 2(b)는 신뢰할 수 있는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역을 나타낸 것이다. 이 경우는 침입자로부터 종단 시스템 및 중간 시스템을 보호하는 방식이다. 모든 중간 시스템에서는 종단 시스템과 동등한 보호서비스가 제공되므로 전송 데이타의 인증, 무결성 그리고 기밀성 여부를 알 수 있으나 한 중간 시스템이 침입자로부터 노출될 경우 전송 데이타의 모든 내용이 노출되는 단점이 있다. 따라서 모든 중간 시스템에서는 인증, 무결성 그리고 비밀보장 서비스에 관련된 모든 정보들을 안전하게 관리해야 하는 구현상 어려움이 발생한다. SP3과 NLSP에서 전송되는 데이타의 PDU(protocol data unit) 구조는 그림 3과 같다. 그림 3의 PDU에서 ICV(integrity check

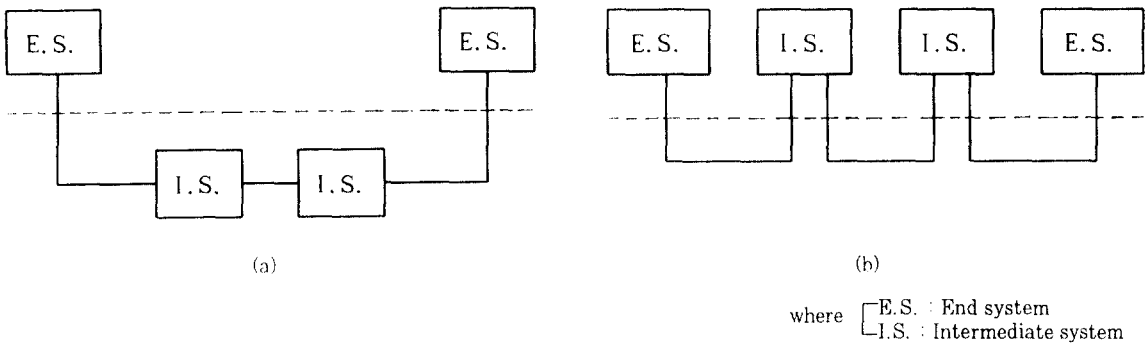


그림 2. SP3과 NLSP에서의 인터네트워크 보호 영역
(a) 신뢰할 수 없는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역
(b) 신뢰할 수 있는 중간 시스템으로 접속된 경우의 인터네트워크 보호영역
Fig. 2. The protection boundary of internetwork in SP3 and NLSP.
(a) The protection boundary with untrusted intermediate system.
(b) The protection boundary with trusted intermediate system.

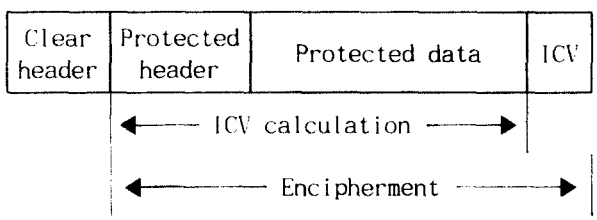


그림 3 SP3과 NLSP에서의 PDU 구조
Fig. 3. The PDU structure in NLSP and SP3.

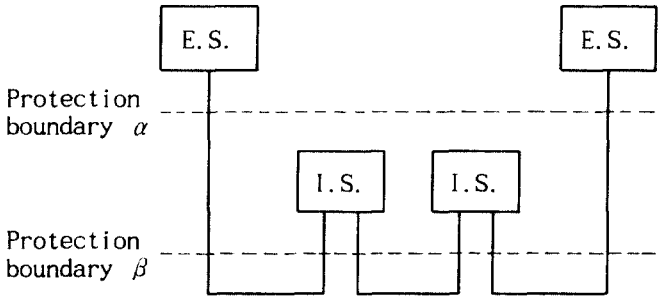


그림 4. 제안한 인터네트워크 보호영역
Fig. 4. The proposed protection boundary in internetwork.

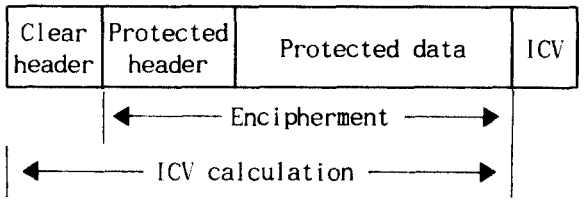


그림 5. 제안한 인터네트워크 보호 시스템을 위한 PDU 구조
Fig. 5. The PDU structure for the proposed security system in internetwork.

value) 영역은 무결성 검사를 위한 영역이며 암호화 영역은 비밀성을 제공하는 영역이다.

본 논문에서는 인터네트워크의 특성을 고려하여 그림 4와 같이 2중화 보호영역을 제안한다. 그림 4에서 보호영역 α는 통신자간의 비밀성을 제공하는 영역이다.

인터네트워크에서 중간 시스템은 최종 통신자가 아니므로 전송데이타의 내용을 노출시킬 필요가 없다. 따라서 인터네트워크의 중간 시스템에서는 비밀보장 서비스를 제공하지 않아도 된다. 그림 4에서 보호영역 β는 네트워크상에서 인증 및 무결성을 제공하는 영역이다. 인터네트워크에서는 각 네트워크에서 전송할 수 있는 데이타의 최대 전송크기(MTU, maximun transmission unit)를 다르게 규정하므로 단편화 과정이 이루어지고 중간 시스템에서는 전송 단편들의 인증 및 무결화 과정이 필요하다. 이러한 중간 시스템에서의 인증 및 무결성 서비스는 각 네트워크에서 전송 데이타의 투명성을 제공하므로 네트워크 상에서 트래픽 양을 감소시킬 수 있다.

제안한 보호영역에서 그림 3의 기존 PDU를 사용할 경우 네트워크상에서 단편화 과정이 발생하면 중간 시스템에서는 암호화 영역을 복호할 수 없으므로 수신된 PDU의 ICV 영역을 검사할 수 없으며 전송할 단편들의 무결성 검사를 위해 ICV 영역을 재 설정해야 하는 문제가 발생한다. 따라서 제안한 보호체계에 적합한 PDU를 그림 5와 같이 제시한다. 그림 5에서 PDU는 보호영역을 먼저 암호화 한후 전체 PDU에 대해 무결성 검사를 하여 ICV 영역을 발생한다. 제안한 보호영역에서 종단 시스템간에는 비밀보장 서비스를 제공하며 중간 시스템에는 비밀보장 서비스를 제공하지 않으므로 중간 시스템에서 전송 데이타의 내용을 알 수 없다. 무결성 서비스는 중간 시스템에서도 제공할 수 있으므로 네트워크 상에서 단편화 과정이 일어날 경우에도 무결성 서비스를 제공할 수 있다.

Ⅲ. 무결성 프로토콜

인터네트워크에서 전송 데이타의 무결성 서비스를 제공하는 대표적인 방식은 DA(delayed authentication) 프로토콜이 있으며 MTU(maximum transmission unit) 프로토콜을 이용한 프로토콜과 키 종속 해쉬 함수를 이용한 프로토콜도 가능하다. 이러한 프로

토콜들을 적용하는 네트워크는 다음과 같은 성질을 갖는다.

- 호스트(host)들은 독립적이다.
- 구성 네트워크들은 게이트웨이에 의해 연결된다.
- 모든 정보는 데이타그램으로 흐른다.

본 논문은 인터네트워크에서 무결성 서비스를 제공하기 위하여 다음과 같은 가정을 한다.

- 패킷은 단편화될 수 있다.
- 같은 패킷의 단편들은 다른 경로를 가질 수 있다.
- 같은 패킷의 단편들은 순서에 상관없이 도착할 수 있다.
- 호스트 간에 전송되는 패킷들은 헤더 영역에 있는 순서 번호에 의해 유일하게 확인된다.
- 선택사항은 패킷의 헤더 영역에 나타낼 수 있다.

1. DA 프로토콜

Tsudik에 의해서 제안된 DA 프로토콜(7)에서의 가정은 다음과 같다.

- 데이타 서명은 일방향 특성함수를 적용한 결과로서 계산된다.
- 패킷의 데이타 서명에 사용된 특성함수는 모든 패킷 단편들의 개개의 데이타 서명으로 재생될 수 있는 함수를 사용한다.
- 송신 호스트(Hsrc)와 수신 호스트(Hdst) 사이에 이동하는 같은 패킷의 모든 단편들은 경로 상에서 같은 지점인 송신 게이트웨이와 수신 게이트웨이를 반드시 통해야 하는 조건 외에는 동적 경로가 적용된다.

DA 프로토콜에서는 전송 패킷이 인증 게이트웨이 상에서 패킷 단위로 무결성 과정을 수행하며 절차는 다음과 같다.

1) 한 게이트웨이가 한 단편(FP_i)을 수신할때 이 패킷의 다른 단편이 처리되었음을 확인하기 위하여 표($H_{src}, H_{dst}, PK_{id}$)를 검사한다. 만약 이 패킷의 다른 단편이 처리되지 않았으면 표에 새로 기록한다.
2) 단편의 서명($F_{char}(FP_i)$)을 계산한다.
3) 한 단편이 전체 패킷을 구성하면 서명값 $F_{char}(FP_i)$는 헤더에 있는 서명값 $F_{char}(P)$와 비교한다. 만약, 두 값이 일치하면 그 단편은 전송되고 표의 기록영역을 없애며 두 값이 일치하지 않으면 그 단편을 버린다.
4) 만약, 단지 한 단편이면 다음의 두 경우가 발생한다.
   - 마지막 단편인 경우, 송신 게이트웨이는 과거에 처리된 모든 단편이 조합된 서명과 헤더에 있는 전체 패킷의 서명을 비교한다. 만약, 그 값이 일치하면 단편은 전송되고 일치하지 않으면 단편은 버려진다. 결과에 관계없이 표의 기록영역은 없어진다.
   - 마지막 단편이 아닌 경우, 송신 게이트웨이는 단편의 길이, 부분 서명 그리고 offset를 표에 저장한다. 그리고 단편은 전송된다.

DA 프로토콜에서 패킷의 마지막 단편이 인증 게이트웨이에 도착하여 전체 패킷의 서명값과 단편들의 조합된 서명값을 비교하며 그 값이 일치하지 않으면 마지막 단편은 버린다.

수신측 호스트에서는 특정시간 내에 패킷의 단편이 도착하지 않으면 재배열 큐에 있는 패킷의 단편들을 무시한다. 따라서 수신측 호스트에서 패킷의 재배열이 이루어지지 않는다. 이 프로토콜은 송신측 호스트에서 데이타 서명 계산을 제외하고는 호스트의 어떤 변경도 요구되지 않는다. 이 프로토콜의 예로는 MAC(message authentication code) 및 MDC(modification detection code) 방식을 이용한 것들이 있다.[7]

2. MTU 프로토콜을 이용한 무결성 프로토콜

MTU 프로토콜을 이용한 무결성 프로토콜은 가정이 없으며 게이트웨이에서 상태정보를 요구하지 않지만 호스트 레벨의 프로토콜 변경이 있어야 하며 패킷의 크기가 줄어들고 상대적으로 패킷 오버헤더가 증가한다. 이 프로토콜은 송신 호스트가 전송 패킷을 단편없이 목적 호스트까지 도달할 수 있는 최대 패킷 크기를 결정해야 하며 최대 패킷 크기가 결정되면 전송 데이타의 서명값을 부가하여 데이타를 전송한다. 게이트웨이는 한 패킷을 수신하면 패킷의 서명을 계산하며 헤더에 있는 서명값과 비교한다. 만약, 두값이 일치하면 패킷은 전송되고 일치하지 않으면 패킷을 버린다.

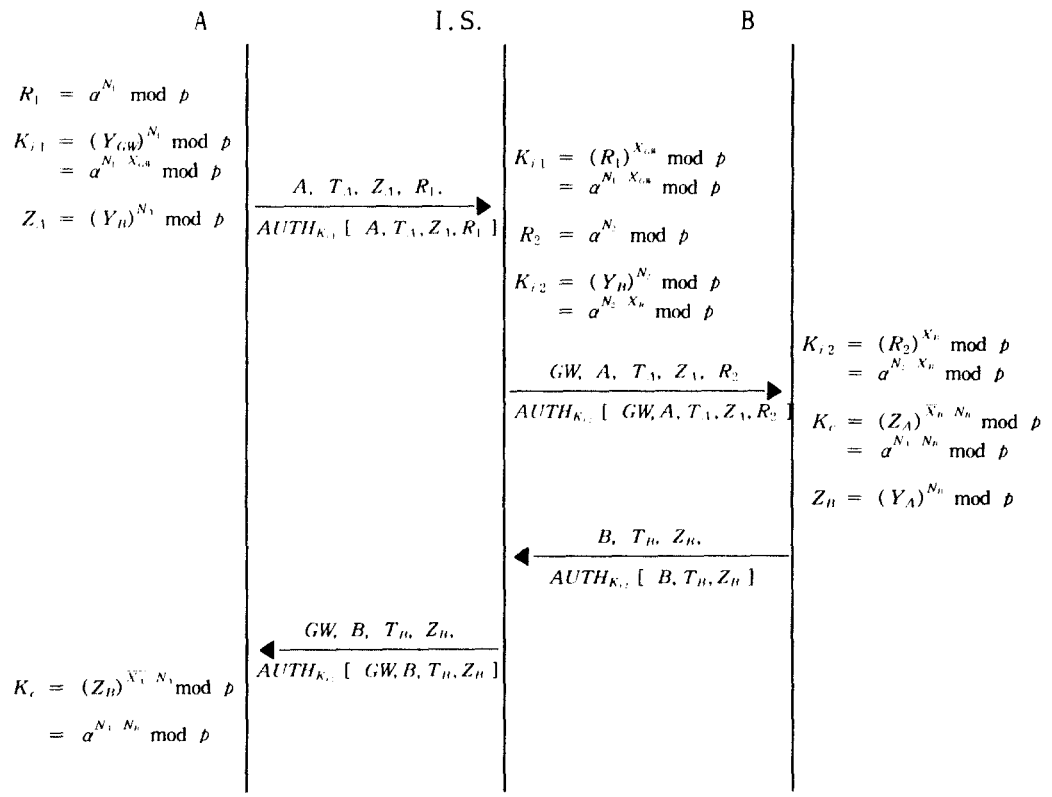
Kent와 Mogul에 의해 제안된 MTU probing 프로토콜[8]의 절차는 다음과 같다. 특별한 PROBE 패킷을 전송하며 각 중간 게이트웨이는 그 네트워크 영역의 MTU를 기록한다. PROBE가 목적 호스트에 도착하면 목적 호스트는 최소 MTU를 송신 호스트에게 알린다. 이 프로토콜은 주어진 경로상에서 단편화가 일어나지 않으나 probing을 제공하기 위하여 모든 게이트웨이에서 프로토콜 변경이 있어야 하며 모든 중간 게이트웨이에서

PROBE 패킷의 처리부하가 발생한다.

3. 키 종속 해쉬 함수를 이용한 프로토콜

DA 프로토콜과 MTU 프로토콜을 이용한 무결성 프로토콜이 인증 게이트웨이 상에서 패킷 단위로 전송 데이타의 무결성을 검사하는 것과는 달리 본 절에서는 인증 게이트웨이 상에서 키 종속 해쉬 함수를 이용하여 패킷의 단편 단위로 무결성 검사를 수행하는 프로토콜을 제시한다. 이 프로토콜은 인증 게이트웨이 상에서 한 패킷의 어떤 단편이 무결성 검사에 실패할 경우 이후의 단편들은 전송하지 않으므로 네트워크 상에서 트래픽 양이 감소하는 장점이 있다. 또한 인증 게이트웨이에서 버퍼가 요구되지 않는다. 이 프로토콜에서 각 단편에 대한 서명값은 일방향 해쉬 및 암호화를 수행함으로써 이루어지며 인증 게이트웨이에서의 절차는 다음과 같다.

1) 한 게이트웨이가 한 단편을 수신할때 이 패킷의 다른 단편이 처리되었음을 확인하기 위하여 표(Hsrc,Hdst,PKid)를 검사한다. 만약 이 패킷의 다른 단편이 처리되지 않았으면 표에 새로운 영역을 만든다.
2) 단편의 서명이 계산되며 헤더에 있는 서명값과 비교한다. 만약, 두 값이 일치하면 단편은 전송되고 일치하지 않으면 단편과 표의 영역을 버리며 동일 패킷의 다른 단편이 도착해도 이를 버린다.
3) 단편이 한 패킷의 마지막 단편인 경우 2)번의 절차가 수행되며 표의 영역을 없앤다.



where, A, B : User, K_c : Confidentiality key,
GW : Gateway, K_{i1}, K_{i2} : Intergrity key,
T_A, T_B : Time stamp,
N_A, N_B, N_1, N_2 : Random number,
$AUTR_{k_{i1}}[A, T_A, V_A, R_1] = E_{k_{i1}}[FHASH(A, T_A, V_A, R_1)]$

그림 6. 인터네트워크에서 인증 기능을 갖는 키 분배 프로토콜
Fig. 6. The key distribution protocol with an authentication function in internetwork.

Ⅳ. 키 분배 프로토콜

암호화 방법에는 크게 대칭 키 암호화 방법 및 비대칭 키 암호화 방법이 있다. 대칭 키 암호화 방법은 처리속도가 빠르고 구현이 간단하나 키 관리가 문제된다. 비대칭 키 암호화 방법은 처리속도가 상대적으로 느리지만 키 관리 및 인증의 기능을 효과적으로 수행할 수 있다. 따라서 일반적으로 정보보호를 위한 암호화 시스템의 구현에서 키 분배에는 비대칭 암호화 방법을 이용하고 이 분배된 암호화 키를 사용하여 전송 데이타의 암복호에는 대칭 키 암호화 방법을 이용한다.

본 논문에서는 무결성 키 분배를 위하여 ElGamal 방식[9]을 비밀보장 키 분배를 위하여 Matsumoto-Imai 방식[10]을 이용하여 본 논문에서 제안한 인터네트워크 보호영역 모델에 적합한 인증 기능을 갖는 키 분배 프로토콜을 그림 6과 같이 제안한다.

키 분배 프로토콜의 절차는 다음과 같다.

1. 종단 시스템 A는 랜덤 수 N_1, N_A와 time stamp T_A를 발생하고 무결성 검사 키 발생에 사용될 R_1, 무결성 검사 키 K_{i1}, 비밀보장 키 발생에 사용할 Z_A를 계산한다. A의 상태 값, T_A, Z_A, R_1, 그리고 인증값을 중간 시스템에게 전송한다. 인증값인 $AUTH_{K_{i1}}\{A, T_A, Z_A, R_1\}=E_{K_{i1}}\{FHASH\{A, T_A, Z_A, R_1\}\}$이다. 여기서, $FHASH\{\ \}$는 단방향 해쉬함수이며 $E_{K_{i1}}\{\ \}$는 키 K_{i1}에 의한 암호화 함수이다.

2. 중간 시스템은 전송된 R_1에 자신의 비밀키를 사용하여 무결성 검사 키 K_{i1}를 구한후 인증값을 검증한다. 인증값이 맞으면 종단 시스템 B와 사용될 무결성 검사 키를 발생하기 위하여 랜덤수 N_2를 발생하고 무결성 검사 키 발생에 사용될 R_2 및 무결성 검사 키 K_{i2}를 계산한다. 중간 시스템의 상태값 GW, T_A, Z_A, R_2 그리고 인증값을 종단 시스 템 B에게 전송한다.

3. 종단 시스템 B는 T_A를 검사하여 최종 도착지까지 허용시간내에 데이타의 도착 여부를 확인하고 무결성 검사 키 K_{i2}를 구한후 수신된 인증값을 검증한다. 종단 시스템 B는 수신된 Z_A를 이용하여 비밀보장에 사용할 키 K_c를 구하고 랜덤 수 N_B를 발생하여 비밀보장 키 발생에 사용할 Z_A를 계산한다. 자신의 상태값 B, time stamp T_B, 비밀보장 키 발생에 사용할 Z_B, 그리고 인증값을 중간 시스템에게 전송한다.

4. 중간시스템은 무결성 검사 키 K_{i2}를 이용하여 수신된 인증값을 검증한 후 자신의 상태 값인 GW와 B, T_B, Z_B 그리고 인증값을 종단 시스템 A에게 전송한다.

5. 종단 시스템 A는 T_B를 검사하여 최종 도착지까지 허용 시간내에 데이타의 도착 여부를 확인한 후 K_{i1}를 이용하여 수신된 인증값을 검증한다. 수신된 Z_B를 이용하여 비밀보장에 사용할 키 K_c를 구한다.

Ⅴ. 분석 및 결과

1. 보호영역 모델 분석

· 종단 시스템간에서만 보호서비스를 설정한 모델 (그림 2(a))

이 모델은 인터네트워크의 중간 시스템에 어떠한 보호서비스도 제공하지 않으므로 구현은 간단하나 네트워크 상에서 전송 데이타의 인증 및 무결성 여부를 알 수 없으므로 인터네트워크를 위한 보호체계로 적합하지 않다.

· 종단 및 중간 시스템에 동일한 보호서비스를 설정한 모델 (그림 2(b))

이 모델은 인터네트워크의 중간 시스템에서 전송 데이타의 인증 및 무결성 여부를 알 수 있으므로 네트워크 상에서 트래픽 양은 감소할 수 있다. 그러나 이 모델은 인터네트워크의 중간 시스템에서 비밀보장 서비스도 제공되므로 한 중간 시스템이 침입자로부터 노출될 경우 모든 전송데이타가 노출된다. 따라서 모든 중간 시스템에서는 인증, 무결성 그리고 비밀보장 서비스에 관련된 모든 정보들을 안전하게 관리해야 하는 구현상 어려움이 발생한다.

· 본 논문에서 제안한 모델 (그림 4)

이 모델은 인터네트워크의 중간 시스템에서 전송 데이타의 인증 및 무결성 여부를 알 수 있으므로 네트워크 상에서 트래픽 양이 감소할 수 있다. 또한, 이 모델은 인터네트워크의 중간 시스템에서 비밀보장 서비스가 제공되지 않으므로 구현이 비교적 간단하고 중간시스템이 노출될 경우에도 비밀보장 키는 노출되지 않으므로 안전하다.

2. 무결성 프로토콜 분석

본 논문에서는 인터네트워크 상에서 무결성 서비스를 제공하는 대표적인 프로토콜인 DA 프로토콜 및 MTU 방식을 이용한 프로토콜을 기술하였으며 키 종속 해쉬

함수를 이용하여 무결성 서비스를 제공하는 프로토콜을 제시하였다. 이 프로토콜들은 아래의 성질들을 사용하여 비교,분석한다.

· 게이트웨이 상에서의 인증 단위
DA 프로토콜 및 MTU 방식을 이용한 프로토콜은 패킷 단위로 인증이 이루어지며 키 종속 해쉬 함수를 이용한 프로토콜은 전송 패킷의 단편 단위로 인증이 이루어진다.

· 게이트웨이 상에서의 순간 인증
DA 프로토콜은 게이트웨이 상에서 단편들이 패킷을 구성할때까지 인증이 일어나지 않는 반면 키 종속 해쉬 함수를 이용한 프로토콜과 MTU 방식을 이용한 프로토콜은 전송 데이타에 대해 순간 인증이 가능하다.

· 단편화 제공
MTU 방식을 이용한 프로토콜은 전송 패킷의 크기가 전체 경로의 최소 MTU 크기 내에 있으므로 게이트웨이 상에서 단편화 과정이 발생되지 않으나 DA 프로토콜과 키 종속 해쉬함수를 이용한 프로토콜은 게이트웨이 상에서 단편화 과정이 발생한다.

· 게이트웨이 및 호스트 변경
MTU 방식을 이용한 프로토콜은 호스트 및 게이트웨이에서 프로토콜 변경이 있다. DA 프로토콜과 키 종속 해쉬 함수를 이용한 프로토콜은 전송 패킷의 데이타 서명 계산을 제외하고는 호스트의 어떠한 변경도 없으나 게이트웨이 상에서는 프로토콜 변경이 있다.

· 전송 패킷 수
DA 프로토콜과 키 종속 해쉬 함수를 이용한 프로토콜은 인증 게이트웨이에서 단편화를 허용하므로 전송 패킷의 수는 증가하지 않으나 MTU 방식을 이용한 프로토콜은 전송 패킷의 크기가 전체 경로의 최소 MTU 크기 내에 있어야 하므로 전송패킷의 수가 증가한다.

· 패킷 크기
세가지 프로토콜 모두 인터네트워크 상에서 데이타 서명값을 전송하기 위한 부가적인 영역이 필요하다.

· 제어 패킷 교환
DA 프로토콜과 키 종속 해쉬 함수를 이용한 프로토콜은 제어 패킷 교환 과정이 필요하지 않으나 MTU 방식을 이용한 프로토콜은 새로운 경로가 설립될 때마다 MTU를 통보하는 제어 패킷이 필요하다.

· 게이트웨이 상에서의 버퍼 요구
DA 프로토콜은 패킷 단위 인증을 위해서 단편의 서명값을 저장하는 버퍼가 필요하나 MTU 방식을 이용한 프로토콜 및 키 종속 해쉬 함수를 이용한 프로토콜은 순간 인증이 일어나므로 버퍼가 요구되지 않는다.

위의 분석에서 키 종속 해쉬 함수를 이용한 프로토콜은 인터네트워크 상에서 호스트 및 게이트웨이의 프로토콜 변경 및 부하가 적을 뿐 아니라 순간 인증 방식으로 전송 데이타에서 공격이 있었던 단편을 바로 검출할 수

표 1. 인터네트워크에서 세가지 네트워크-레벨 무결성 방식의 비교
Table 1. Comparision of three network-level integrity scheme in internetwork.

Integrity protocol / Characteristics	MTU probing	DA	Key-dependent hash
Authentication unit	paket	paket	fragnent
Instant authentication	yes	no	yes
Fragmentation support	no	yes	yes
Gateway modification	yes	yes	yes
Host modification	yes	no	no
More packets generated	yes	no	no
Packet size increased	yes	yes	yes
Control packets needed	yes	no	no
Buffer in gateway	yes	yes	no

표 2. 80486(50MHz) PC에서 대표적인 보호 알고리듬의 수행시간
Table 2. Excution time of the representative security algorithm on a 50MHz 80486 based PC.

Algorithm	Excution time (ms)	Note
DES	2.05	input : 64 bit output : 64 bit
MDS	2.34	input : 512 bit output : 128 bit
Montogomery	3.10	512 bit multiplication

있으므로 네트워크 상에서 트래픽 양을 줄일 수 있다. 따라서 키 종속 해쉬 함수를 이용한 프로토콜은 인터네트워크에서 무결성 서비스를 제공하는 적합한 프로토콜이라 할 수 있다. 표 1은 본 논문에서 기술한 세가지 무결성 방식을 서로 비교한 것이다.

3. 키 분배 프로토콜의 구현

제안한 키 분배 프로토콜은 모듈라 연산을 위하여 Montgomery 알고리듬[11]을 그리고 인증값 계산을 위하여 MD5(message digest 5)[12] 및 DES(data encryption standard)[13] 알고리듬을 이용하여 구현하였다. 이 알고리듬들의 80486 PC(50MHz)에서 수행시간은 표 2와 같다.

Ⅵ. 결 론

본 논문에서 제안한 인터네트워트 보호영역 모델은 종단 시스템간에는 비밀성이 유지되며 종단 시스템과 중간 시스템간 그리고 중간 시스템들간에 인증 및 무결성이 제공되는 모델이다. 따라서 본 모델은 인터네트워크의 중간 시스템에서 비밀보장 서비스가 제공되지 않으므로 구현이 비교적 간단하고 중간 시스템이 노출될 경우에도 비밀보장 키는 노출되지 않으므로 안전하다. 본 논문에서 제시한 키종속 해쉬 프로토콜은 인터네트워크상에서 무결성 서비스를 제공하는 방식으로 기존의 DA 프로토콜 및 MTU 방식을 이용한 프로토콜에 비해 중간 및 종단 시스템에서 프로토콜 변경 및 부하가 적을 뿐 아니라 순간 인증 방식으로 전송 데이타에서 공격이 있었던 단편을 바로 검출할 수 있으므로 네트워크 상에서 트래픽 양을 줄일 수 있다. 본 논문에서 제안한 키 분배 프로토콜은 제안한 인터네트워크 보호모델에 적합하며 식별자를 사용함으로써 인증기능을 갖는다. 본 키 분배 프로토콜에서는 무결성을 위한 키를 분배하기 위하여 일방 간접 인증 기능을 갖는 one-pass 메카니즘인 ElGamal 방식을 이용하며 비밀보장을 위한 키를 분배하기 위하여 D-H형 방식을 이용하였다. 또한, DES, MD5 및 Montgomery 모듈라 곱 알고리듬들을 이용하여 제안한 키 분배 프로토콜을 소프트웨어적으로 구현하였다.

참고문헌

1. Douglas E. Comer, *Internetworking with TCP/IP*, Prentice Hall, 1991.
2. ISO, *Information Processing - Open System Interconnection - Basic Reference Model - Part 2 : Security Architecture*, ISO 7498-2, 1989.
3. ITU-T/ISO/IEC, *Information Technology - Open Systems Interconnection - Network Layer Security Protocol*, International Standard, November. 1993.
4. R.Hinden, *Internet Protocol Version6 (IPv6) Specification*, Internet Draft, Octorber. 1994.
5. Randall Atkinson, *IPv6 Security Architecture*, Internet Draft, November. 1994.
6. SDNS Program Office, *Security Protocol 3(SP3)*, SDN.301, Revision 1.5, May. 1989.
7. Gene Tsudik, "Datagram Authentication in Internet Gateways: Implications of Fragmentation and Dynamic Routing," *IEEE JSAC*, Vol. 7, No. 4, May. 1989.
8. C. Kent and J. Mogul, "Fragmentation Considered Harmful," *ACM SIGCOMM*, August. 1987.
9. T. El-Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. on inform.* Theory, Vol. IT-31, July. 1985.
10. T. Matsumoto, Y. Takashima, and H. Imai "On Seeking Smart Public-Key-Distribution Systems," *IEICE Trans.*, Vol. E69, No. 2, February. 1986.
11. P. Montgomery, "Modular Multiplication Without Trial Division," *Maths. of Computation*, Vol.44, No.170, pp.519-521, April. 1985.
12. R.Rivest, *The MD5 Message Digest Algorithm*, Request for Comments(RFC) 1321, 1992.
13. NBS, *Data Encryption Standard*, U.S. FIFP PUB 46, pp.1-18, January. 1977.

朴 暎 昊(Young Ho Park) 정회원

1966년 10월 17일생
1989년 2월: 경북대학교 전자공학과 (공학사)
1991년 2월: 경북대학교 전자공학과 (공학석사)
1995년 8월: 경북대학교 전자공학과 (공학박사)

※주관심 분야: 컴퓨터 네트워크 및 암호이론

文 相 在(Sang Jae Moon) 정회원

1948년 4월 20일생
현재 : 경북대학교 전자공학과 교수
한국통신학회 논문지 제19권 제4호 참조