OSI 트랜스포트 계층을 위한 보호 시스템의 개발

°김기현*, 박영호*, 문상재*, 박정수**, 신명기**, 강신각**
* 경북대학교 전자공학과
** 한국전자통신연구소

The development of security system for OSI transport layer

°Ki-hyun Kim*, Young-ho Park*, Sang-jae Moon*, Jung-soo Park**, Myung-ki Sin**, Shin-Gak Kang**
* Dept. of Electronics, Kyungpook National University
** Electronics and Telecommunications Research Institute

요약문

개방형 시스템에서 사용자에게 안전성 및 신뢰성을 보증하기 위하여 정보 보호가 필요하다. 본 논문에서는 트랜스포트 계층에서 보호 서비스를 제공하기 위하여 ISO와 IEC에서 표준으로 권고하고 있는 TLSP와 SA-P를 분석하고, 표준에서는 정의하지 않았으나 구현상 필요한 세부 사항들을 정의한다. 그리고 구현 모델을 제시하고 이에 기초하여 보호 시스템을 개발한다. 개발을 위한 환경으로는 USL의 ONP를 사용한다.

1. 서론

개방형 시스템(open system)간의 통신을 보호하기 위하여 ISO에서는 OSI 참조 모델내에 보호 구조인 ISO 7498-2[1]를 제공하고 있다. OSI 참조 모델에서 보호 서비스 제공을 위한 계층별 적용을 고려해 보면, 먼저 응용 및 프리젠테이션과 같은 상위 계층에서의 보호는 응용 서비스 요소나 특별한 응용의 활용도에 의존하므로 각 응용별로 구현해야 하는 번거로움이 있다. 반면에 네트워크 레벨에서의 보호는 각 개별망에 종속적이며 보호 비용이 많이 든다. 이와는 달리 트랜스포트 계층에서의 보호는 하위 망의 형태와는 독립적이므로 망의 특성과는 무관하게 사용자에게 보다 유연성있는 보호 서비스를 제공하는 장점이 있으며 부인봉쇄 서비스를 제외한 모든 보호 서비스를 제공한다.

트랜스포트 계층에서 보호 서비스를 제공하기 위하여 NSA(national security agency), NIST(national institute of standards and technology)와 DCA(defense communication agency)에서는 SDNS(secure data network systems) 프로젝트를 수행하여 SP4(security protocol 4)[2]를 정의하고 있으며, 이를 기초로 하여 ISO와 IEC에서는 트랜스포트 계층 보호 프로토콜(TLSP, transport layer security protocol)[3]의 표준화 중이다. 또한 두 트랜스포트 객체간에 보호 연관 속성을 공유하기 위하여 트랜스포트 계층 보호 프로토콜의 일부분으로써 보호 연관 프로토콜(SA-P, security association - protocol)[4]을 권고하고 있다.

본 논문에서는 종점간 사용자 데이타의 보호를 위하여 트랜스포트 계층에서 TLSP와 SA-P를 이용하여 보호 시스템을 개발한다. 보호 시스템 개발을 위하여 먼저 TLSP와 SA-P를 분석하고, 표준에서는 권고하지 않았으나 구현상 필요한 세부 사항들을 정의한다. 그리고 구현 모델을 제시하고, 이 모델에 기초하여 보호 시스템을 개발한다. 개발을 위한 OSI 트랜스포트 계층 환경으로는 ONP(open network platform)[5-8]를 사용한다. 보호 알고리듬으로는 비밀보장 서비스를 제공하기 위하여 DES(data encryption standard)[9]를 사용하고 무결성 서비스를 제공하기 위하여 SHA(secure hash algorithm)[10]를 사용한다. 그리고 KTE(key token exchange)를 수행하기 위하여 Diffie-Hellman 키 분배 알고리듬[11]을 사용하고 인증 기능을 지원하기 위하여 DSS(digital signature standard)[12]를 사용한다.

2. 트랜스포트 계층 보호 프로토콜

TLSP는 ISO/IEC 8073[13]및 ISO 8602[14]의 확장이며, 접속 및 비접속형 TPDU (transport protocol data unit)의 전송에 대한 데이타 보호 및 비보호를 허용한다. TLSP는 ISO 7498-2에서 명시하는 트랜스포트 계층 보호서비스인 대등실체 확인, 데이타 발신처 확인, 접근제어, 접속 비밀보장, 비접속 비밀보장, 복구기능을 갖는 접속 무결성, 복구기능이 없는 접속 무결성 그리고 비접속 무결성 서비스들을 제공한다. TLSP는 암호화 메카니즘을 사용하여 이 서비스들을 지원하고, 보호 라벨링(labeling), 키 및 식별자와 같은 보호 속성은 보호 관리에 의해 미리 설정되거나 보호연관 프로토콜을 사용하여 설정된다. 키의 재설정은 보호연관 프로토콜이나 프로토콜의 외적 수단을 통하여 지원된다.

그림 1과 2는 OSI 참조모델에서의 접속 및 비접속 TLSP의 위치를 나타낸다. 그림에서 트랜스포트 계층은 TPDU를 구성하는 상위부분과 네트워크 계층과 네트워크 계층 서비스를 사용하여 TPDU를 전송하는 하위부분으로 구분되며, TLSP는 상위부분과 하위부분 사이에 위치한다. TLSP는 접속형 트랜스포트 프로토콜과 비접속형 트랜스포트 프로토콜이 모두 같은 형태이며 운용은 네트워크 서비스 형태에 독립적이다. 그러나 제공되는 서비스들은 트랜스포트 프로토콜의 형태에 의존한다.

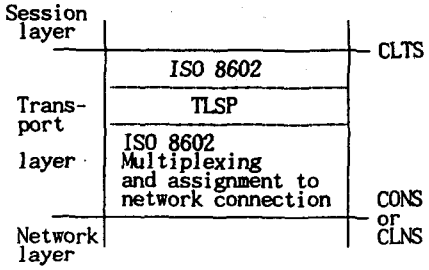

Fig. 1. TLSP with ISO 8602

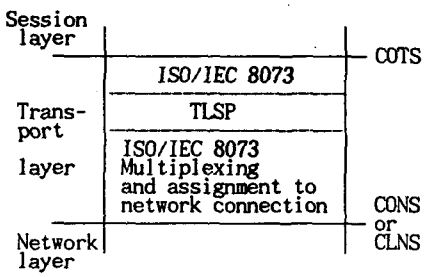

Fig. 2. TLSP with ISO/IEC 8073

2.1 보호 연관 속성

TLSP의 처리는 보호연관에 의하여 결정되며 각 트랜스포트 객체들은 이 연관들을 공유한다고 가정한다. 각 보호연관은 각 종단 시스템에서의 속성집합에 의하여 정의되며, 보호연관 식별자 SA-ID는 통신을 보호하는데 사용될 수 있는 연관들의 집합을 식별한다. 보호속성들은 상호교환 및 ASSR(agreed set of security rule)을 통하여 설정된다. ASSR은 사용되는 보호 메카니즘을 규정하는 공통된 규칙들의 집합이며, 상호 동의하여 정의할 필요가 있는 모든 파라미터들을 포함한다. 보호 규칙과 식별자는 제 3자에 의해 등록될 수 있다.

TLSP의 보호 연관 속성들은 다음과 같다.

- o SA(security association) identification
- o Indicator
- o Address of peer TLSP entity(s)
- o Identifier for the agreed set of security rules
- o Protection QOS selected for the SA
- o Mechanisms selected for the SA
- o Label mechanism attributes
- o ICV mechanism attributes
- o SN(sequence number) mechanism attributes
- o EXSN mechanism attributes
- o Encipherment mechanism attributes

2.2 TLSP의 기능

TLSP는 TPDU를 보호연관 속성에 기초하여 보호하며 SE TPDU(security encapsulation TPDU)로 캡슐화(encapsulation) 한다. 캡슐화 기능은 접속/비접속 비밀보장 및 무결성 서비스를 제공하기 위하여 암호화와 무결성 검사 기능를 결합하여 사용한다. 또한 캡슐화 기능은 네트워크 접속의 할당 및 멀티플렉싱(multiplexing)을 제외한 트랜스포트 계층의 모든 프로토콜 처리 기능을 수행한 후에 적용된다. decapsulation은 디멀티플렉싱(demultiplexing) 후와 다른 프로토콜 처리 기능을 수행하기 전에 수행된다. TLSP의 기능은 데이타 암호화 기능, 무결성 기능, 보안 라벨 기능, 보호 페딩 기능, 대등 실체 인증 기능 및 보호연관 기능으로 나눌 수 있다. SE TPDU 수신측에서는 보호 연관 속성에 의해서 규정된 모든 보호의 존재 여부를 검증한다. 부적당하게 보호된 TPDU는 무시된다.

표 1은 TLSP 기능들이 실제로 구현될 때 트랜스포트 각 등급에서 포함되어지는 상황을 나타낸다.

Table 1. TLSP elements of procedure in transport protocol class

Protocol mechanism	ISO/IEC 8073 class					ISO 8602
	0	1	2	3	4	
Cryptographic confidentiality	m	m	m	m	m	m
ICV processing	m	m	m	m	m	m
Direction indicator processing	*	*	*	*	*	*
Unique sequence number	NA	NA	o	o	o	NA
Peer address check processing	*	*	*	*	*	*
Security labels for cryptographic assoc.	o	o	o	o	o	o
Connection release	o	o	o	o	o	NA
Key replacement	o	o	o	o	o	o

* Procedure always include in class
NA Not applicable
O Negotiable procedure whose implementation in equipment is optional
m Negotiable procedure whose implementation in equipment is mandatory

2.3 SE TPDU의 구조

SE TPDU는 클리어 헤드, 암호화 동기, 보호된 내용 및 ICV 영역으로 구성된다. 그림 3은 SE TPDU의 구조를 나타내고 있다.

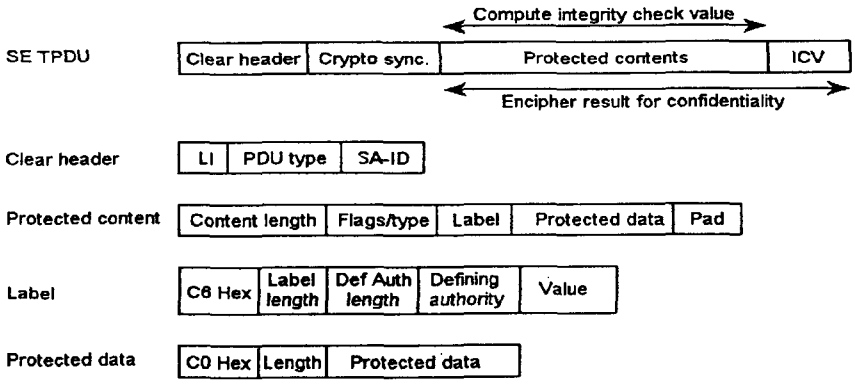

Fig. 3. Structure of the SE TPDU

3. 보호 연관 프로토콜

두 통신 객체간에 통신 보호를 제어하는 정보의 집합이 보호 연관이며, TLSP의 처리를 위하여 두 트랜스포트 객체는 보호 연관 속성을 공유해야 한다. 통신 객체 사이에 협상을 통하여 동일한 보호 속성 정보를 공유하는 과정을 보호 연관의 설정이라 한다. 보호 연관을 설정하는 방법에는 TLSP를 사용하기 전에 보호 관리에 의해 미리 설정하는 방법과 보호 연관 프로토콜을 사용하는 방법이 있다.. ISO와 IEC의 JTC1/SC6에서는 트랜스포트 계층 보호 프로토콜의 일부분으로써 보호 연관 프로토콜을 권고하고 있으며, 이 보호 연관 프로토콜은 SA 설정, 유지 및 중지/해제를 수행하기 위하여 비대칭 메카니즘을 사용한다. 보호 연관 프로토콜은 TLSP 객체들에게 두 객체간의 상호인증, SA 속성들의 초기화 그리고 무결성및 비밀보장을 제공하기 위한 초기 정보의 설정 기능을 제공한다.

보호 연관을 설정하기 이전에 각 트랜스포트 객체는 지원하는 메카니즘, 각 비대칭 알고리듬에 대한 비대칭 키 쌍, TA(trusted authority)의 확인표, 그리고 TA의 공개키와 이 공개키를 이용하는 비대칭 알고리듬과 같은 정보를 미리 설정해야 하며, 이러한 정보의 사전 설정은 보호정책에 따라 결정된다.

3.1 SA-P의 논리적 기능

SA-P의 논리적 기능은 KTE(key token exchange), 상호인증, 보호 속성 협상 및 보호 연관 중지/해제를 수행하는 4가지 기능으로 분류되며 다음과 같다.

첫째, TLSP 객체들은 공유할 비밀값을 생성하기 위하여 KTE를 수행한다. TLSP 객체들은 공유 비밀값과 비밀키 알고리듬을 사용하여 KTE 이후의 나머지 SA-P에 대한 비밀보장을 제공하며, 이 공유 비밀값은 보호 연관의 키와 ISN 속성 협상시 참조열로 사용된다. 둘째, SA를 설정하는 동안 TLSP 객체는 다른 TLSP 객체를 인증하기 위하여 확인표와 디지탈 서명[15]을 교환한다. 이 기능을 수행하기 위하여 인증 확인표와 공개키 쌍이 필요하다. 세째, 보호 연관 속성을 협상하기 위하여 PDU를 교환한다. SA 속성 협상에는 서비스 협상, 라벨 협상, 키와 ISN 선택, 키 대체, 그리고 그 밖에 필요한 SA 속성 협상이 있다. 네째, 보호 연관을 중지 또는 해제를 위하여 PDU를 교환한다.

3.2 보호 연관의 설정 및 해제 절차

SA-P의 4가지 논리적 기능은 프로토콜에서 SA PDU를 교환함으로써 수행된다. 첫번째 교환은 키 토큰 교환이며 암호화를 적용하지 않는다. 두번째 교환은 보호된 보호연관 협상으로 구성되며 인증을 제공한다. 마지막으로 보호 연관의 중지 및 해제를 위하여 교환 기능이 제공된다.

3.2.1 보호 연관의 설정

TLSP 객체나 로컬 보호 관리자가 보호 연관 설정을 시작할 수 있다. 시작하는 TLSP 객체는 아래 기능들을 수행한 후 다음과 같은 정보를 포함하는 SA PDU를 수신 TLSP 객체로 전송한다.

a) 선택한 보호 연관 식별자

b) 키 토큰 1

c) 두번째 SA-P 교환을 보호하기 위해 사용되는 비밀보장 및 무결성 메카니즘

여기서 비밀보장 메카니즘은 대칭키 암호화 알고리듬과 이의 동작 모드를 말하며, 무결성 메카니즘이란 비대칭 암호화 알고리듬과 이와 관련된 디지탈 서명을 의미한다.

보호 연관 요청 PDU 수신시, 수신 TLSP 객체는 개시자가 제안한 보호 메카니즘에 대해 수용 가능한 메카니즘을 선택한다. 이때 수용 가능한 메카니즘이 한 가지도 없는 경우 보호 연관의 거절 및 이유를 알리기 위한 SA PDU를 보내다. 적절한 메카니즘을 선택하였으면 자신의 보호 연관에 대한 식별자를 선택하고 KTE를 수행한 후 다음과 같은 정보를 포함하는 SA PDU를 개시자에게 보낸다.

a) 선택한 보호 연관 식별자

b) 키 토큰 2

c) 선택한 비밀보장 및 무결성 메카니즘

보호 연관 요청에 대한 첫번째 응답 PDU 수신시,. 시작하는 TLSP 객체는 인증 및 보호 연관 속성을 협상하기 위한 두번째 SA PDU를 전송한다. 이때 SA PDU에는 다음과 같은 정보가 포함된다.

a) 상대의 보호 연관 식별자(보호 연관 헤더부분에 포함)

b) 확인표

c) 보호 서비스들의 목록

d) 보호 라벨 집합

e) 키 및 ISN 포인터 집합

f) 그 밖의 SA 속성들

위에서 상대의 보호 연관 식별자를 제외한 나머지 정보는 SA PDU의 내용 영역에 들어가며 이 정보에 대하여 개시자의 비밀키로 디지탈 서명을 하고 첫번째 교환에서 생성된 세션키로 내용 영역을 암호화하여 전송한다.

개시자로부터 두번째 SA PDU를 수신한 응답자는 첫번째 교환에서 생성된 세션키로 내용 영역을 복호화한 후 수신한 확인표와 디지탈 서명을 검증하고 제안된 보호 서비스, 보호 라벨, 키/ISN 및 그 밖의 보호 속성에 대하여 그 수용 여부를 검사한다. 이중 한 항목이라도 검사에 실패하면 보호 연관 설정에 대한 거절과 그 이유를 포함한 SA PDU를 개시자에게 전송한다. 모든 검사를 통과한 경우, 응답자는 제안된 보호 서비스, 보호 라벨, 키/ISN 및 그 밖의 보호 속성에 대하여 적절한 것을 선택한 후 다음과 같은 항목을 포함하는 SA PDU를 개시자에게 전송한다.

a) 상대의 보호 연관 식별자(보호 연관 헤더에 포함)

b) 확인표

c) 선택된 보호 서비스

d) 보호 라벨 집합 중에서 선택된 subset

e) 키와 ISN

위에서 상대의 보호 연관 식별자를 제외한 나머지 정보는 SA PDU의 내용 영역에 들어가며 이 정보에 대하여 개시자의 비밀키로 디지탈 서명을 하고 내용 영역을 암호화하여 전송한다.

3.2.2 SA 해제/중지

TLSP 객체 또는 로컬 보호 관리자가 SA 해제/중지를 시작한다. SA 해제/중지하는 시작자는 SA 수립의 시작자가 될 필요는 없다. SA 해제/중지 요구 및 응답을 위한 SA PDU는 확인표와 SA 해제/중지 이유 영역을 내용 영역으로 구성하고, 이 내용 영역에 대하여 디지탈 서명과 암호화를 수행한 후 전송한다.

3.3 SA PDU의 구조

SA PDU는 프로토콜 식별자, PDU 길이, PDU 형태, SA-ID, SA-P 형태 및 SA PDU 내용영역으로 구성되어 있다. 그림 4는 SA PDU 구조를 나타내고 있다. KTE와 디지탈 서명 메카니즘을 사용하는 SA-P에서 SA 내용 영역은 교환 ID, 내용 길이 및 내용 영역으로 구성된다.

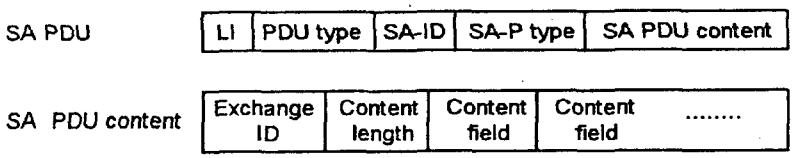

Fig. 4. Structure of the SA PDU

4. 트랜스포트 계층의 보호 시스템 구성

4.1 보호 모델

그림 5는 TLSP와 SA-P의 구현 모델을 나타내고 있다. 트랜스포트 객체가 트랜스포트 계층 사용자로부터 서비스를 요청받으면, 트랜스포트 객체는 그 서비스를 지원해 준다. 만약 보호 서비스가 요구된다면 트랜스포트 객체는 TLSP 객체에게 보호 서비스를 요청하며 TLSP 객체는 TLSP와 SA-P를 이용하여 트랜스포트 객체에게 보호 서비스를 제공해 준다.

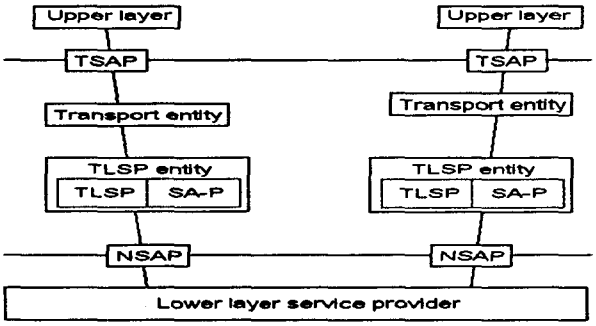

Fig. 5. TLSP implementation model

4.2 보호 관리 정보

두 통신 객체간에 TLSP를 통하여 보호 서비스를 제공받기 위해, 두 통신 객체는 암호 알고리듬, 암복호 키, 인증 기법 및 보호 레이블과 같은 정보를 사전에 공유하여야 한다. 이 공유 정보는 보호 연관 PDU의 교환과 ASSR을 통하여 설정된다. 본 논문에서는 이들 보호 관리 정보에 대하여 ASSR, SA-P 정보, 및 TLSP 정보로 구분하여 SMIB로 구성하였다.

공유 정보들은 보호 연관 설립 과정을 통해 교환되는데, 보호 연관을 설립할 때마다 모든 정보를 전송하여 협상하는 것을 피하기 위하여 ASSR을 이용한다. 보호 연관 설립 과정에서 개시자는 여러개의 ASSR 식별자를 전송하며, 응답자는 하나를 선택하게 된다. 본 논문에서는 두 통신자간에 ASSR을 미리 공유하고 있다고 가정하였으며, 한개의 ASSR 식별자만을 이용하였다. 그림 6[4,16]은 구현에 사용한 ASSR의 예를 나타내고 있다.

```
a) ASSR-ID : 1.0014.13.5.111

b) Selected definition module
   (PE or DO) Auth: none, low, high
   AC           : none, low, high
   Confid       : none, low, high
   Integ        : none, low, high
c) Security Label
   - Sensitivity level
     (Unclass, Integrity, Confidentiality, Secret)
     · Label->sensitivity = Unclass
       implies
            Auth = none, AC = none, Confid = none, Integ = none
     · Label->sensitivity = Integrity
       implies
            Auth = none, AC = none, Confid = none, Integ = high
     · Label->sensitivity = Confidentiality
       implies
            Auth = none, AC = none, Confid = high, Integ = none
     · Label->sensitivity = Unclass
       implies
            Auth = high, AC = high, Confid = high, Integ = high
d) Mechanism module - security labels for access control
   for security service selected: AC = high or Conf = high
   Label_Def_Auth      : XYZ
   Explicit indication : Yes
e) Protection of all service parameters
   for security service selected: Integ = high or Conf = high
f) Mechanism module - Integrity Check Value
   for security service selected: Integ > none or Auth = high
                  or Mechanism security label(Confid = high)
   ICV_Alg_ID   : XYZ
   ICV_Blk_size : x octets
   Rekey after  : 10,000 PDUs
   Key distribution mechanism: asymmetric
g) Mechanism module - Integrity sequence number
   for security service selected: Integ = high or Auth = high
   ISN_Len      : 4 octets
h) Mechanism module - Encipherment
   for security service selected: Conf > low
   Enc_Alg_ID   : XYZ
   Enc_Blk_size : x octets
   Rekey after  : 10,000 PDUs
   Key distribution mechanism: asymmetric
i) Mechanism module - Connection authentication
   for security service selected: AC > low or PE Auth > low
   Enc_Alg_ID   : XYZ
   Enc_Blk_size : x octets
   Key distribution mechanism: asymmetric
j) Mechanism module - Asymmetric key distribution
   for mechanism encipher or integrity check value
   PKC_Alg_ID   : RSA
```

Fig. 6. ASSR

SA-P 정보는 SA-P를 수행하기 위하여 두 통신자간에 공유되어야 할 정보를 나타낸다. SA-P 정보는 지원하는 메카니즘, 확인표, TA의 공개키, 그리고 TA의 공개키를 이용하는 비대칭 알고리듬 등을 포함하고 있다. 이 값들은 앞의 ASSR 값들처럼 미리 공유하고 있다고 가정하였다. 마지막으로 TLSP 정보는 SA-P를 통해 협상된 보호 연관 속성을 나타낸다.

그림 7은 위에서 분류한 보호 관리 정보와 SA-P/TLSP와의 관계를 나타내고 있다.

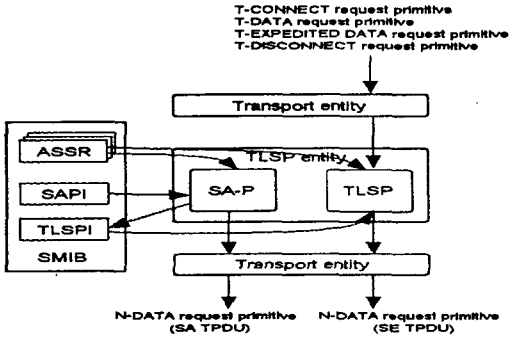

Fig. 7. The relation among security management information, SA-P, and TLSP

4.3 SA-P와 TLSP의 구성

TLSP 객체는 보호 연관을 설정, 유지, 변경 및 해제하기 위하여 보호 연관 설정을 위한 첫번째 SA PDU, 보호 연관 설정을 위한 두번째 SA PDU, 보호 연관 중지/해제를 위한 SA PDU, 그리고 키 대체를 위한 SA PDU들을 교환한다. 본 논문에 위의 4가지 SA PDU를 그림 8과 같이 구성하였다.

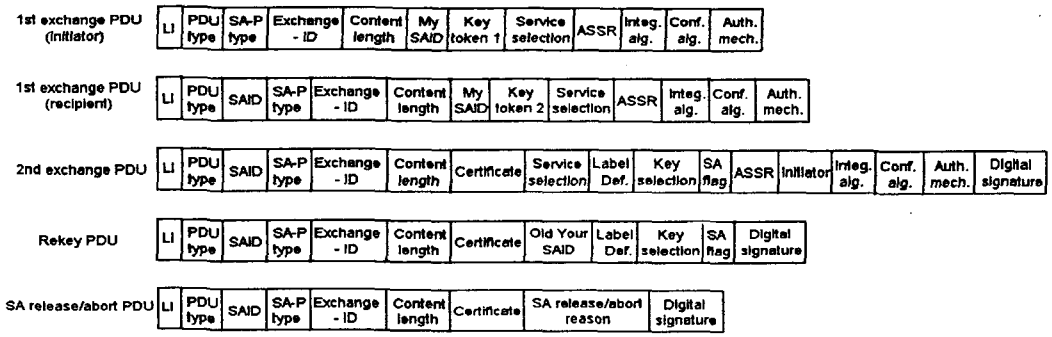

Fig. 8. Structure of the SA PDU

그림 9는 접속 지향 트랜스포트 프로토콜에서의 순서제어를 나타내고 있다. TLSP 객체가 트랜스포트 객체로 부터 접속 요구를 받으면, TLSP 객체는 SA-P를 이용하여 보호 연관을 설정하고 이를 SMIB에 저장한다. 그리고, TLSP 객체는 보호 연관 속성에 기초하여 트랜스포트 객체로 부터의 모든 TPDU를 보호한다.

송신 절차는 TLSP 요구 프리미티브를 처리하는 과정이며 TLSP 객체는 보호 연관 속성들을 가진 SMIB로 접근할 수 있다. 만약 보호 연관 속성이 존재하지 않을 경우 SA-P를 이용하여 보호 연관을 설정한다. 보호 연관이 SMIB 내에 존재할 경우, 보호 헤드, 무결성을 위한 ICV, 비밀보장을 위한 암호화

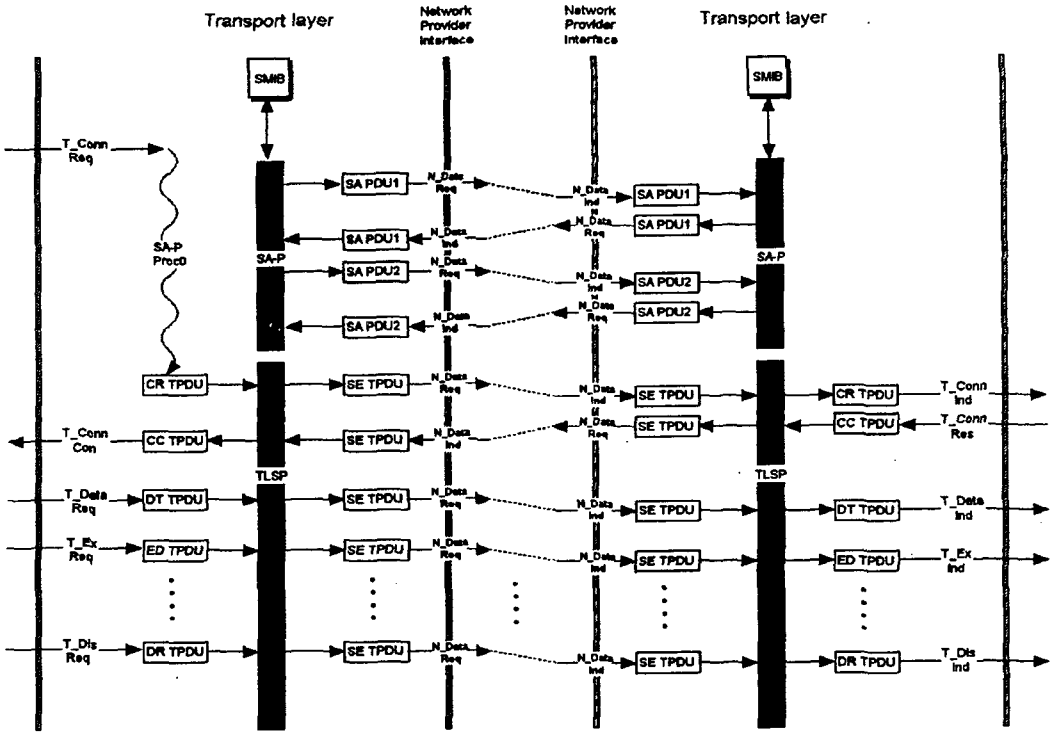

Fig. 9. Connection-oriented TLSP flow

를 한 후 비보호 헤드를 붙여 SE TPDU로 캡슐화 한다. 그리고 UN(underlying network) 요구 프리미티브를 형성하여 하위 네트워크로 전달한다. 수신절차는 하위 네트워크로 부터의 지시 프리미티브를 수신하면, PDU 형태를 검사한다. SA PDU일 경우 SA-P를 이용하여 보호 연관을 설정하거나 해제한다. SE TPDU일 경우, 프리미티브의 인자와 SAID를 이용하여 SMIB내의 보호 연관을 찾아 PDU에 적절한 메카니즘을 적용한다. 먼저 비보호 헤드 영역을 제거하고, PDU를 보호화하고 ICV를 검사한다. 그리고 TLSP 지시 프리미티브는 지정된 스택으로 가게 된다.

4.4 보호 알고리듬

보호 알고리듬으로는 비밀보장 서비스를 제공하기 위하여 DES를 사용하고 무결성 서비스를 제공하기 위하여 SHA를 사용하였다. 그리고 KTE를 수행하기 위하여 Diffie-Hellman 키 분배 알고리듬을 사용하고 SA-P 인증 기능의 디지탈 서명을 지원하기 위하여 DSS를 사용하였다.

4.5 구현

OSI 참조 모델에 기초한 개방 시스템의 환경 구축과 이에 따른 실험을 돕기 위하여 UNIX의 등록사인 USL(UNIX system laboratory)의 ONP(open network platform)을 사용하였다. ONP는 UNIX system V용으로 설계된 네트워킹 프로그램, 도구(tool) 및 응용(application)의 집합으로서 개방 시스템 응용의 설계, 개발 그리고 실험을 위한 실험적 환경을 제공한다. ONP가 UNIX system V 용으로 개발된 이유는 장기적으로 볼 때 OSI 환경의 운용체계에 알맞으며, 이식(potable)과 기능 향상(upgradable)이 용이하고 표준 응용 서비스를 제공하기 때문이다. ONP의 하드웨어/소프트웨어 요소들은 크게 다음과 같이 구분된다.

- 응용 서비스 라이브러리(application service library)
- 기본 스택 프로토콜(core stack protocol)
- 서브네트워크 프로토콜(subnetwork protocol)

본 논문에서는 ONP WAN/LAN 트랜스포트 패키지 중 그림 10과 같이 ONP LAN 트랜스포트를 구성하고 TLSP와 SA-P를 이식시켜 구현하였다. ONP LAN 트랜스포트는 CLNP 상에 TP4로 구성되어 있으며, 멀티플레싱 및 디멀티플렉싱 기능을 제외한 등급 4의 모든 기능을 제공한다.

TLSP와 SA-P를 구현하기 위한 접근 방식으로서 TLSP와 SA-P를 트랜스포트 계층의 부계층으로 구성하고 TLSP 객체는 트랜스포트 객체로 부터의 모든 TPDU에 대하여 캡슐화하는 방법을 도입하였다. 본 논문에서는 트랜스포트 계층의 부계층으로 TLSP와 SA-P를 삽입하기 위하여 그림 10의 ONP LAN 트랜스포트 드라이버에서 네트워크 계층 서비스를 사용하여 TPDU를 전송하는 기능을 수행하는 함수인 tp4_sendpdu()와 N_DATAinducation()에 TLSP와 SA-P를 지원하는 함수인 tlsp_provider() 루틴을 추가함으로서 인터페이스 하였다.

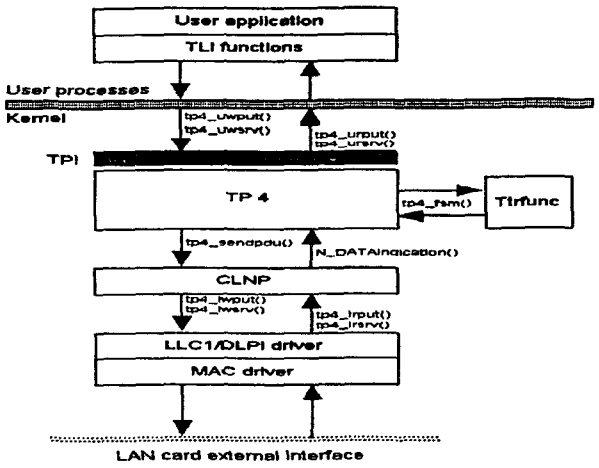

Fig. 10. ONP LAN transport driver

5. 실험 및 고찰

트랜스포트 계층 보호 프로토콜의 수행은 응용 계층 객체들에 의해 이루어지고, 응용 계층 객체들에는 사용자, 키 관리와 시스템/보호 관리 응용 객체가 있다. 본 논문에서는 SA-P를 이용한 보호 연관 협상과 TLSP를 이용한 화일 전송을 시뮬레이션하였다. ASSR과 보호 연관 정보는 두 통신 객체가 서로 공유하고 있다고 가정하였다.

5.1 보호 연관 협상 및 해제

시뮬레이션의 첫번째 과정은 키 토큰 교환이며 이때 분배된 키는 다음 PDU 교환의 암복호화 키로 사용된다. 다음은 인증 및 SA 속성 협상 과정으로 여기서 협상된 보호 연관 속성들은 TLSP를 지원하며 SMIB에 저장된다. 그림 11은 협상된 보호 연관 속성들의 예를 나타내고 있다.

그 후, 분배된 키와 SMIB 내의 저장된 속성들에 따라 보호 서비스가 제공되어 데이타 전송이 일어난다. 데이타 전송이 끝나고 보호 연관 중지/해제 요구를 받으면, TLSP 객체는 SA-P를 이용하여 보호 연

- SA Identification
  - Local_SAID: 61616161
  - Peer_SAID : 61616162
  - SAID_Len : 4
- Initiator : 00
- Peer_Adr : 490001000050cf48b01
- ASSR_ID : 01.14.0014.13.05.111.
- Protection QOS selected for the SA
  - QOS_Label : 0 AC : 2
  - DOAuth : 0 CLConf: 0
  - CLInt : 2 PEAuth: 2
  - COConf : 2 COInt : 0
  - COIntr : 0
- Mechanisms selected for the SA
  - Label : 01 Conf : 01
  - ICV : 01 SN : 01
  - PEAuth: 01 UNPort: 00
- Label mechanism attributes
  - Label_Ref : 167
  - Label_Def_Auth : 7a
  - Label_Content : f400c6050302020202
- ICV mechanism attributes
  - ICV_Alg : 25
  - ICV_Len : 160
  - ICV_Blk : 0
  - ICV_Kg : 0
  - ICV_Gen_Key :
  - ICV_Check_Key :
- SN mechanism attributes
  - Data_Local_SN : f34a182a
  - Data_Peer_SN : e8691a5f
- EXSN mechanism attributes
  - Data_Local_EXSN : 63fc058b
  - Data_Peer_EXSN : e883a149
- Encipherment mechanism attributes
  - Enc_Alg : 1e
  - Enc_Blk : 64
  - Enc_Kg : 0
  - Enc_Key : 69b24dcea4a00ac9
  - Dec_Key : 93822a24dbe5a45e
- User define
  - Local_SN : f349f11a
  - Peer_SN : e868f34f
  - Local_EXSN : 63fbde7b
  - Peer_EXSN : e8837a39
  - EX_ICV_Gen_Key :
  - EX_ICV_Check_Key:
  - EX_Enc_Key : f266150ca5f9a591
  - EX_Dec_Key : 28cd2f8d34f48276
  - Auth_Mch : 13
  - Auth_Gen_Key : 93822a24dbe5a45e
  - Auth_Check_Key : 6c97937a79b30a86

Fig. 11. Negotiated SA attributes

관 중지 및 해제를 한다. 보호 연관 중지일 경우 TLSP 객체는 보호 서비스를 중단하고 보호 연관 속성들을 SMIB에 저장한다. 보호 연관 해제일 경우 TLSP 객체는 보호 서비스를 중단하고 보호 연관 속성들을 SMIB에 저장하지 않고 버린다.

5.2 데이타 전송 시뮬레이션

TLSP 객체는 SA-P를 이용하여 초기화된 보호 연관 속성에 기초하여 보호 서비스를 지원한다. 데이타 전송 시뮬레이션을 위하여 사용한 메세지는 "This program supports the development of OSI transport security protocol and application."이며 DT TPDU는 다음과 같다.

04f000018054686973207072 6f6772616d20737570706f72747320746865206465766c6f706d656e74206f6
6204f5349207472616e73706f72742073656375726974792070726f746f636f6c20616e64206170706c696361
74696f6e

아래는 데이타 전송 시뮬레이션의 한 예로써 위 DT TPDU의 처리 과정을 나타낸다.

단계 1: UNPort를 검사한다. 만약 UNPort가 TRUE이면 TLSP를 처리하지 않는다.

단계 2: SA-P에서 협상된 보호 연관 속성값들을 읽어들인다.

단계 3: SN = TRUE이면 순서번호를 검사한다.

단계 4: 보호 데이타 영역을 구성한다. 이 영역의 값은 다음과 같다.

c0dd04f000018054686973207072 6f6772616d20737570706f72747320746865206465766c6f706d656e7
4206f66204f5349207472616e73706f72742073656375726974792070726f746f636f6c20616e6420617070
6c696361746 96f6e

단계 5: Label = TRUE이면 라벨 영역을 구성한다. 이 영역의 값은 다음과 같다.
c68b817a00f4c6050302020202

단계 6: 플래그 영역을 구성한다. 이 영역의 값은 00이다.

단계 7: ICV = TRUE이면, ICV 페드 영역을 구성한다. SMIB의 ICV_Blk = 0이므로 이 영역의 값은 없다.

단계 8: 보호 데이타, 라벨, 플래그 및 ICV 페드 영역을 포함하는 보호 내용 영역을 구성한다. 이 영역의 값은 다음과 같다.
ed00c68b817a00f4c6050302020202c0dd04f000018054686973207072 6f6772616d20737570706f72747320746865206465766c6f706d656e74206f66204f5349207472616e73706f727420736563757269747920726f746f636f6c20616e64206170706c69636174696f6e

단계 9: ICV = TRUE이면, ICV 영역을 구성한다. 여기서 사용된 무결성 알고리듬은 SHA이며, ICV 영역 값은 다음과 같다.
693e1c6ad4e05153cb38c3eda6dd341eb8f4aa4e

단계 10: Conf = TRUE이면 보호내용 영역과 ICV 영역을 암호화 한다. 여기서 사용된 비밀보장 알고리듬은 DES이며 필요하다면 암호화 페딩 영역을 구성한다. 암호화된 영역 값은 다음과 같다.
e6b0cd6578916166c9f51c6768c7abaddb64dfe300930662668337f65d55424d616d3651728c7b7c7eb46a1334b586b769b5516e636980fb68be756d3c6cd6605619220c4db067eb7acf7165d76fc3657202578a80feffe262a447c212a206a666e42a22598508616af152984140ac4210aac3143150a997cf2d859ed04f0c6fab5ee61e85d854bf

단계 11: 만약 요구된다면 암호화 동기 영역을 구성한다. 이 영역의 값은 1e1e1e1e이다.

단계 12: 클리어 헤더 영역을 구성한다. 이 영역의 값은 054861616162이다.

단계 13: 클리어 헤더, 암호화 동기, 보호 내용, 및 ICV 영역을 포함하는 SE TPDU를 구성한다. 구성된 SE TPDU는 다음과 같다.
0548616161621e1e1e1eee6b0cd6578916166c9f51c6768c7abaddb64dfe300930662668337f65d55424d616d3651728c7b7c7eb46a1334b586b769b5516e636980fb68be756d3c6cd6605619220c4db067eb7acf7165d76fc3657202578a80feffe262a447c212a206a666e42a22598508616af152984140ac4210aac3143150a997cf2d859ed04f0c6fab5ee61e85d854bf

TLSP 객체가 SE TPDU를 수신하여 송신 과정의 역과정을 수행한 후에 같은 전송 메세지를 얻을 수 있었다.

6. 결론

본 논문에서는 종점간 사용자 데이타의 보호를 위하여 트랜스포트 계층에서 TLSP와 SA-P를 이용하여 보호 시스템을 개발하였다. 보호 시스템의 개발을 위하여 먼저 TLSP와 SA-P를 분석하고, 표준에서는 권고하지 않았으나 구현에 필요한 세부 사항들을 정의하였다. 그리고 구현 모델을 제시하여 개발하고, 보호 시스템이 제공하는 보호 서비스와 기능을 실험하였다. 개발 환경으로는 ONP를 사용하였다.

보호 시스템은 SA-P를 이용한 보호 연관 설정 과정과 TLSP를 이용한 보호 데이타 교환과정으로 구성하였다. 먼저, SA-P를 통하여 두 TLSP 객체간의 상호인증, SA 속성들의 초기화 그리고 무결성 및 비밀보장을 제공하기 위한 초기 정보의 설정 기능을 제공하였다. 보호 연관 설정 과정이 끝난 후 TLSP를 이용하여 대등 실체 인증, 비밀보장, 무결성과 접근제어 서비스가 제공되면서 정보가 교환됨을 확인하였다.

보호 알고리듬으로는 DES를 사용하여 비밀보장 서비스를 제공하고, SHA를 사용하여 무결성 서비스를 제공하였다. 그리고 Diffie-Hellman 키 분배 알고리듬을 사용하여 KTE를 수행하고, DSS를 사용하여 SA-P 인증 기능의 디지탈 서명을 지원하였다. 이를 통하여 실험한 보호 시스템은 표준에서 제시된 조건을 만족함을 확인하였으며, 통신할 때마다 다른 키를 사용하므로 안전함을 확인하였다.

참고문헌

[1] ISO/IEC 7498-2, *Information Processing Systems - OSI Basic Reference Model - Part 2 Security Architecture*, 1989.

[2] *Formal Description of the SDNS Security Protocol at Layer 4 (SP4)*, NIST, 1992. 3.

[3] ISO/IEC 10736, *Transport Layer Security Protocol*, 1993. 10.

[4] ISO/IEC 10736/AM1, *Transport Layer Security Protocol - Amendment 1: Security Association Establishment*, 1993.10.

[5] *Open Network Platform (ONP) OSI LAN Transport Release 2.0 Programmer's Guide*, 1991.

[6] *Open Network Platform (ONP) OSI LAN Transport Release 2.0 Adminstrator's Guide*, 1991.

[7] *Open Network Platform (ONP) OSI Lower Layer Services for: LAN Transport Release 2.1, WAN Transport Release 1.2 Programmer's Guide (Version 0)*, 1993.

[8] *Open Network Platform (ONP) Lower Layer Provider Interface (Version 0)*, 1993.

[9] National Bureau of Standard, *Data Encryption Standard*, U.S. FIPS PUB 46, pp. 254-264, 1977.

[10] National Institutes Standard Technology, *Specification for a Secure Hash Standard (SHS)*, FIPS YY Draft, January 1992.

[11] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. on Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[12] National Institute Standard Technology, *Specification for a Digital Signature Standard (DSS)*, FIPS XX Draft, August 1991.

[13] ISO/IEC 8073, *Protocol for providing the Connection-mode Transport Service*, 1993.

[14] ISO/IEC 8072, *Transport service definition for Open System Interconnection*, 1993.

[15] ISO/IEC 9594-8, *Authentication Framework*, 1990. 12.

[16] ITU-T Q2317 X.802, *Lower Layer Security Model*, 1993. 10.

[17] ISO/IEC 11577, *Network Layer Security Protocol*, 1993. 11.

[18] *NISTIR 4614 Standard Security Label for GOSIP*, An Invitational Workshop.

[19] ISO/IEC 11570, *Information technology - Telecommunication and information exchange between systems - Open System Interconnection - Transport protocol identification mechanism*, 1992. 12.

[20] Warkwick Ford, *Computer Communication Security - Principles, Standard Protocols, and Techniques*, Prentice Hall, 1994.

[21] 김영희, 강신각, 임주환, OSI 수송계층에서의 보호연계 규약, 한국통신정보보호학회 종합학술발표회 논문집 제3권 1호, 1993.11.