분산 네트워크상에서 다중등급보안 메세지 처리를 위한 네트워크 보안 커널의 설계

o
홍기용* · 조인준** · 김동규*
컴퓨터공학과* 아주대학교
전산통계학과** 배제대학교

A Design of Network Security Kernel for Multilevel Secure Message Handling on the Distributed Network

o
K. Y. Hong* · I. J. Jo** · D. K. Kim*
Department of Computer Engineering* AJOU University
Department of Computer Science** Pai-Chai University

요 약

본 논문에서는 다중 등급의 기밀성을 갖는 메세지의 보호를 위한 보안 특성 함수와 보안 오퍼레이션을 제시하였으며, 이를 구현하기 위한 네트워크 보안 커널의 구조를 설계하였다. 제안한 네트워크 보안 커널은 분산 네트워크상에서 다중등급보안 메세지를 안전하게 보호할 수 있도록 하는 분리된(Isolated) 보호 기능을 제공한다.

Key words: Security Kernel, Access Control, Multilevel Security, Message Handling System

1. 서론

서로 다른 등급의 기밀성(sensitivity)을 갖는 다수의 컴퓨터 및 네트워크 시스템으로 구성된 분산 네트워크 환경에서 보안 요구사항은 중요한 고려사항으로 인식되어야 한다. 일반적으로 네트워크상에는 안전한 시스템(Trusted Systems)과 안전하지 못한 시스템(Untrusted System)들이 함께 존재하기 때문에, 여러 다른 네트워크들과의 상호 접속이 증가하고 있는 오늘날의 상황에서 안전한 컴퓨터 시스템 자체만으로 네트워크 보안에 대한 해결책을 제공하기에는 불충분하다. 컴퓨터 네트워크상에서 정보 보호를 위하여 NIST, NCSC, ISO/OSI, CCITT, ECMA, 그리고 IEEE등의 기관에서 보안 서비스와 메카니즘에 대한 많은 논의와 그 연구가 진행되고 있다[1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 14, 16]. CCITT는 메시지 처리 시스템 보안에 대하여 CCITT X.400 MHS 권고안을 통하여 안전한 액세스 관리(Secure Access Management and Administration)와 안전한 메시지 처리(Secure Messaging)의 2가지 측면에서 기술하고 있다[3, 4, 5, 8, 12, 14]. 그러나, 안전한 메세지 처리를 위해 X.400에서 보안기능들을 정의하고는 있으나 이를 위한 명백한 모델이나 또는 메카니즘을 제공하고 있지는 못하다. PEM(Privacy Enhanced Mail)과 같은 경우에도 암호화를 통해서만 메세지를 보호할 뿐 액세스 제어에 대해서는 아직 고려하고 있지 않은 실정이다[6, 7, 13, 15].

본 논문에서는 분산 네트워크 환경에서 다중등급의 기밀성을 갖는 메세지를 안전하게 처리할 수 있도록 하는 네트워크 보안 커널의 설계에 대하여 논한다.

2. MHS 보안 개념

MHS에 대한 보안 위협은 위장, 메세지 순서 변경, 정보의 변조, 서비스 거부, 정보 누출, 그리고 서비스 부인 등의 다양한 형태로 나타날 수 있다. X.400 권고안에서는 MHS의 보안을 위하여 두가지 측면을 기술하고 있는데 이들은 안전한 액세스 관리 측면과 안전한 메세지 처리 측면이다[3, 8, 12, 14]. CCITT와 NIST 등의 MHS 보안 기능 정의는 표준화에 따르는 개념적이고 추상화된 내용으로 기술된 것이므로 보다 정형화된 보안 정책의 제시가 필요하며 제시된 보안 정책을 만족하는 보안 메카니즘의 설계 및 구현이 수반되어야 한다.

3. 네트워크 액세스 제어 메카니즘 설계

3.1 네트워크 액세스 제어를 위한 보안 특성

본 절에서는 네트워크 액세스 제어 메카니즘을 위한 보안 특성들을 제안한다. 제안된 보안 특성들은 기존의 BLP (Bell-LaPadula) 모델[16]에서 제시한 단순 보안 특성(simple security property), 스타 보안 특성(* security property), 그리고 임의적 보안 특성(discretionary security property)을 포함하며, 또한 네트워크 액세스 제어를 위하여 본 논문에서 새롭게 추가한 접속 보안 특성(connect security property), 흐름 보안 특성(flow security property), 그리고 단순 일치 보안 특성(simple compatibility security property)들로 구성된다.

● 임의적 보안 특성(discretionary security property)

임의적 보안 특성은 액세스 제어 리스트(ACL)와 같은 임의적 액세스 제어 메카니즘을 요구한다. *GetACL(O)*은 객체 *O*의 ACL을 반환하는 함수이다.

$$ds(S, O, m) = \begin{cases} TRUE & if\ m \in M\ \ .and.\ \ \{S,m\} \in GetACL(O) \\ FALSE & otherwise \end{cases}$$

● 단순 보안 특성(simple security property)

이 보안 특성은 주체가 액세스하고자 하는 액세스 모드가 액세스 모드 집합 M에 정의되어 있으며, 또한 주체의 현재 보안 레이블이 객체의 보안 레이블을 지배하는 경우에 판독(r) 액세스를 허용한다. *dom(A, B)*는 보안 레이블 *A*가 보안 레이블 *B*를 지배(dominate)하는가를 판단하는 함수이다. *CSL(S)*는 주체 *S*의 현재 보안 레이블(Current Security Label)을 반환하는 함수이다.

$$ss(S, O, m) = \begin{cases} TRUE & if\ m \in M\ \ .and.\ \ dom(CSL(S), SL(O)) \\ FALSE & otherwise \end{cases}$$

● 스타 보안 특성(* security property)

이 보안 특성은 주체의 객체에 대한 'Write Down' 액세스를 방지하기 위한 것이다. *eqv(A, B)*는 보안 레이블 *A*와 *B*가 서로 같은가를 판단하는 함수이며, 액세스 모드 'r', 'w', 'd'는 각각 판독, 기록, 삭제 액세스를 의미한다.

$$star(S, O, m) = \begin{cases} TRUE & if\ m = 'r'\ \ .and.\ \ dom(CSL(S), SL(O)) \\ TRUE & if\ m = 'w'\ \ .and.\ \ dom(SL(O), CSL(S)) \\ TRUE & if\ m = 'd'\ \ .and.\ \ eqv(CSL(S), SL(O)) \\ FALSE & otherwise \end{cases}$$

이들 기본적인 보안 특성들은 네트워크 환경이 아닌 단일의 컴퓨터 시스템에서의 보안 특성들로 제시된 것이므로, 본 논문에서는 이외에 네트워크 액세스 제어 메카니즘을 위하여 다음과 같은 추가적인 보안 특성들을 제안한다.

● 접속 보안 특성(connect security property)

개시측(Initiator)인 MHS 에이전트의 현재 보안 레이블과 상대측(Target) MHS 에이전트의 보안 레이블의 공통 집합이 개시측 MHS 에이전트의 현재 보안 레이블과 서로 같다면 상호

접속이 가능하다.

$$cs(S1, S2) = \begin{cases} TRUE & if\ eqv(CSL(S1), CSL(S1) \cap SL(S2)) \\ FALSE & otherwise \end{cases}$$

● 흐름 보안 특성(flow security property)

개시측인 MHS 에이전트의 현재 보안 레이블과 상대측 MHS 에이전트의 현재 보안 레이블이 서로 같다면 메세지 객체의 제출, 전송, 또는 배달이 가능하다.

$$fs(S1, S2) = \begin{cases} TRUE & if\ eqv(CSL(S1), CSL(S2)) \\ FALSE & otherwise \end{cases}$$

● 단순 일치 보안 특성(simple compatibility security property)

단순 일치 보안 특성은 단일 등급의 기밀성을 갖는 메세지 스풀 객체와 단일 등급의 기밀성을 갖는 메세지 객체간의 보안성 관계를 정의한 것으로, 메세지 객체의 보안 레이블과 이들을 저장하는 메세지 스풀의 보안 레이블은 서로 동등해야 함을 의미한다.

$$scompat(A, B) = \begin{cases} TRUE & if\ eqv(A, B) \\ FALSE & otherwise \end{cases}$$

3.2 보안 오퍼레이션(Security Operation)의 설계

MHS 네트워크 보안을 위하여 오퍼레이션은 보안 정책을 위반하지 않도록 안전하게 설계되어야만 한다. 본 논문에서, MHS 네트워크 보안을 위해서 설계된 오퍼레이션은 *CreatMsg, ReadMsg, WriteMsg, DeleteMsg, Bind, Submit, Transfer,* 그리고 *Deliver* 이며 다음과 같이 정형적으로 기술된다.

● *CreateMsg* 오퍼레이션

CreateMsg 오퍼레이션은 주체 *S*가 메세지 객체 *O*를 생성하기 위한 것으로 다음과 같이 정의된다.

```
CreateMsg ( S, O, MSPOOL )
Begin
  CSL_S      ← GetCSL ( S );
  SL_MSPOOL  ← GetSL ( MSPOOL );

  if    S ∈ SSET   .and.
        ds( S, MSPOOL , 'w' )   .and.
        ss( S, MSPOOL , 'w' )   .and.
        star ( S, MSPOOL , 'w' )   .and.
        scompat ( SL_MSPOOL , CSL_S )
  then  OSET ← OSET ∪ O;
        SL_O ← CSL_S;
        ∀S ∈ SSET , ACL_O ← ∅;
  endif
End
```

메세지 객체 *O*가 생성되기 위해서는 주체의 현재 보안 레이블과 메세지 객체가 생성되어 저장되어질 메세지 스풀(*MSPOOL*)의 보안 레이블이 같아야 한다. *CreateMsg* 오퍼레이션에 의하여 생성된 메세지 객체 *O*는 객체의 집합 *OSET*에 추가되며 생성된 객체 *O*의 보안 레이블은 주체 *S*의 현재 보안 레이블로 할당된다. 또한, 모든 객체에 대하여 생성된 객체 *O*의 액세스 제어 리스트는 공집합이된다.

● *ReadMsg* 오퍼레이션

ReadMsg 오퍼레이션은 주체 *S*가 메세지 객체 *O*를 판독하기 위한 것으로 다음과 같이 정의된다.

```
ReadMsg (S, O)
Begin
  if    S ∈ SSET .and. O ∈ OSET .and.
        ds (S, O, 'r') .and.
        ss (S, O, 'r') .and.
        star (S, O, 'r')
  then  S reads the contents of O ;
  endif
End
```

MHS 사용자는 오직 이 *ReadMsg* 오퍼레이션을 통하여 메세지를 읽을 수 있다. 이와 같이 주체 *S*가 메세지 객체 *O*를 읽기위하여 요구되는 주체 및 객체간의 보안레이블 관계는 주체의 현재 보안 레이블이 메세지 객체의 보안 레이블을 지배해야 하는 것이다.

● *WriteMsg* 오퍼레이션

WriteMsg 오퍼레이션은 주체 *S*가 메세지 객체 *O*를 기록하기 위한 것으로 첨가 또는 수정에 해당하는 액세스도 이에 포함된다. MHS 사용자는 오직 이 *WriteMsg* 오퍼레이션을 통하여 메세지를 기록할 수 있다.

```
WriteMsg (S, O)
Begin
  if    S ∈ SSET .and. O ∈ OSET .and.
        ds (S, O, 'w') .and.
        ss (S, O, 'w') .and.
        star (S, O, 'w')
  then  S writes to O ;
  endif
End
```

● *DeleteMsg* 오퍼레이션

DeleteMsg 오퍼레이션은 주체 *S*가 메세지 객체 *O*를 삭제하기 위한 것으로 다음과 같이 정의된다. MHS 사용자는 오직 이 *DeleteMsg* 오퍼레이션을 통하여 메세지를 삭제할 수 있다.

```
DeleteMsg (S, O)
Begin
  if    S ∈ SSET .and. O ∈ OSET .and.
        ds (S, O, 'd') .and.
        ss (S, O, 'd') .and.
        star (S, O, 'd') .and.
        ds (S, MSPOOL, 'd') .and.
        ss (S, MSPOOL, 'd') .and.
        star (S, MSPOOL, 'd')
  then  OSET ← OSET - O;
  endif
End
```

● *Bind* 오퍼레이션

Bind 오퍼레이션은 주체 *S1*이 주체 *S2*를 바인드하기 위한 것으로 다음과 같이 정의된다.

```
Bind (S1, S2)
Begin
  CSL_S1    ← GetCSL (S1);
  SL_S2     ← GetSL (S2);

  if     S1, S2 ∈ SSET     .and.
         cs (S1, S2)
  then   SSET      ← SSET ∪ S2;
         OSET      ← OSET ∪ S2;
         CSL_S2    ← CSL_S1 ∩ SL_S2;
  endif
End
```

주체 *S1*이 주체 *S2* 를 바인드하기 위해서 *S1*의 현재 보안 레이블은 *S1*의 현재 보안 레이블과 *S2*의 보안 레이블의 공통 집합과 같아야 한다. 바인드 오퍼레이션의 결과로 *S2*의 현재 보안 레이블은 *S1*의 현재 보안 레이블과 *S2*의 보안 레이블의 공통 집합으로 할당된다.

● *Submit* 오퍼레이션

Submit 오퍼레이션은 주체 *S1*이 수신자 *R*에게 보낼 메세지 객체 *O*를 주체 *S2*에게 제출하기 위한 것으로 다음과 같이 정의된다. 여기서 *S1*은 UA, *S2*는 *MTA*, *O*는 제출코자 하는 메세지 객체, 그리고 *R*은 수신자를 의미한다.

```
Submit(S1, S2, O, R)
Begin
  CSL_S1      ← GetCSL(S1);
  CSL_S2      ← GetCSL(S2);
  SL_R        ← GetSL(R);
  SL_O        ← GetSL(O);
  SL_MSPOOL ← GetSL(MSPOOL);
  if     S1, S2 ∈ SSET   .and.  O ∈ OSET   .and.  R ∈ USET   .and.
         fs(S1, S2)          .and.
         ds(S1, O, 'r')      .and.
         ss(S1, O, 'r')      .and.
         star(S1, O, 'r')    .and.
         scompat(SL_MSPOOL, CSL_S2)   .and.
         ds(S2, O, 'r')      .and.
         ss(S2, O, 'r')      .and.
         star(S2, O, 'r')    .and.
         ds(S2, MSPOOL, 'w')     .and.
         ss(S2, MSPOOL, 'w')     .and.
         star(S2, MSPOOL, 'w')   .and.
         ds(R, O, 'r')       .and.
         ss(R, O, 'r')       .and.
         star(R, O, 'r')
  then   OSET ← OSET ∪ O;
         SL_O ← CSL_S1;
  endif
End
```

● *Transfer* 오퍼레이션

Transfer 오퍼레이션은 주체 *S1*이 주체 *S2*에게 메세지 객체 *O*를 전송하기 위한 것으로 다음과 같이 정의된다. 여기서 *S1*과 *S2*는 MTA를 의미하며 *O*는 전송하고자 하는 메세지 객체를 의미한다.

```
Transfer (S1, S2, O)
Begin
  CSL_S2  ← GetCSL (S2);

  if    S1, S2 ∈ SSET  .and.  O ∈ OSET  .and.
        fs(S1, S2)        .and.
        ds(S1, O, 'r')    .and
        ss(S1, O, 'r')    .and.
        star(S1, O, 'r')  .and.
        scompat (SL_MSPOOL , CSL_S2)  .and.
        ds(S2, O, 'r')    .and.
        ss(S2, O, 'r')    .and.
        star(S2, O, 'r')  .and.
        ss(S2, O, 'w')    .and.
        star(S2, O, 'w')
  then  OSET ← OSET ∪ O;
        SL_O ← CSL_S2;
  endif
End
```

● *Deliver* 오퍼레이션

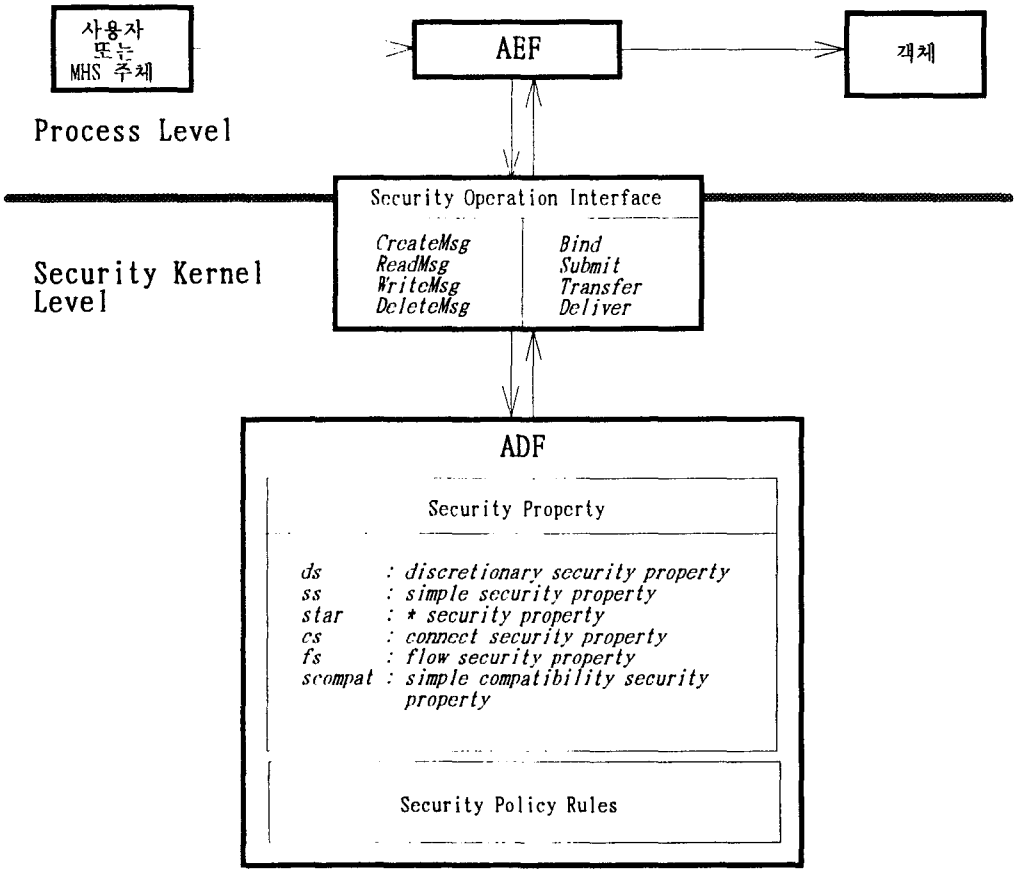
Deliver 오퍼레이션은 주체 *S1*이 주체 *S2*에게 메세지 객체 *O*를 배달하기 위한 것으로 다음과 같이 정의된다. 여기서 *S1*은 MTA를 의미하며, *S2*는 *UA* 또는 *MS*를 의미하며, 그리고 *O*는 배달하고자 하는 메세지 객체를 의미한다.

```
Deliver (S1, S2, O)
Begin
  CSL_S2  ← GetCSL (S2);

  if    S1, S2 ∈ SSET  .and.  O ∈ OSET  .and.
        fs(S1, S2)        .and.
        ds(S1, O, 'r')    .and.
        ss(S1, O, 'r')    .and.
        star(S1, O, 'r')  .and.
        scompat (SL_MSPOOL , CSL_S2)  .and.
        ds(S2, O, 'r')    .and.
        ss(S2, O, 'r')    .and.
        star(S2, O, 'r')  .and.
        ss(S2, O, 'w')    .and.
        star(S2, O, 'w')
  then  OSET ← OSET ∪ O;
        SL_O ← CSL_S2;
  endif
End
```

4 네트워크 보안 커널 구조

이상으로 제시한 보안 특성 함수 및 보안 오퍼레이션을 기반으로 하는 MHS를 위한 네트워크 액세스 제어 메카니즘은 AEF(Access Control Enforcement Facility), 보안 오퍼레이션 인터페이스, 그리고 ADF(Access Control Decision Facility)로 구성되며 그 구조는 다음의 <그림 3-1>과 같다. 사용자 또는 주체의 메세지 객체에 대한 액세스는 AEF를 통하여 이루어지는 것으로, 사용자 또는 주체의 액세스 요구에 해당하는 보안 오퍼레이션을 실행함으로써 액세스 서비스를 제공한다. 이러한 액세스 서비스에 대한 액세스 제어 결정은 ADF를 통하여 이루어지는 것으로, 이 ADF는 액세스 제어 결정을 위하여 보안 정책 규정(Security Policy Rules)을 근간으로 한 보안 특성 함수들의 실행 결과에 의존한다.



AEF : Access Control Enforcement Facility
ADF : Access Control Decision Facility

<그림 3-1> 안전한 MHS를 위한 네트워크 보안 커널 구조

6. 결론

메세지 처리 시스템(MHS : Message Handling System)에서 다중 등급의 기밀성을 갖는 메세지를 안전하게 처리하고 네트워크상에서 정보 흐름을 안전하게 제어하기 위해서는 네트워크 보안 정책과 이를 만족하는 보안 메카니즘이 설계되어야 한다. 이러한 액세스 제어 및 정보 흐름 제어는 암호화 기법을 이용한 정보 보호와는 서로 다른 측면의 정보 보호 기능을 제공하는 것으로 상호 보완적이며 혼합시에 보안성을 높일 수 있게 된다.

본 논문에서는 MHS의 다중 등급 보안(MLS : Multilevel Security)을 위하여 MHS 에이전트인 UA(User Agent), MTA(Message Transfer), 그리고 MS(Message Store)들의 보안에 관련된 액세스 및 오퍼레이션을 정의하고, 네트워크 사용자의 메세지에 대한 액세스 행위가 이들 오퍼레이션을 통하여 안전하게 이루어질 수 있도록 네트워크 액세스 제어 메카니즘을 설계하는 것에 중점을 두었다. 이를 위하여 보안 특성 함수와 보안 오퍼레이션을 정형적으로 제시하였으며, 이러한 보안 특성 함수와 보안 오퍼레이션을 구현하기 위한 하나의 방안으로 네트워크 보안 커널의 구조를 제시하였다. 본 논문에서 제안한 액세스 제어 메카니즘 및 네트워크 보안 커널의 구조는 분산 네트워크상에서 다중등급 기밀 메세지를 안전하게 처리할 수 있는 하나의 해결 방안이 되며, 추후 이를 분산 네크워크상에 구현하고자 한다.

참 고 문 헌

1. National Computer Security Center(NCSC), 'Department of Defense Trusted Computer System Evaluation criteria, Department of Defense,' DoD 5200.28-STD, Washington, D.C., Dec. 1985, pp. 7- 54.
2. National Computer Security Center(NCSC), 'Trusted Network Interpretation of the Department of Defense Trusted Computer System Evaluation criteria,' NCSC-TG-005, Version-1, Washington, D.C., Jul. 1987, pp. 223 - 260.
3. Pietro Schicker, 'Message Handling System, X.400, 'Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elsevier Science Publishers B.V., North-Holland, 1989, pp. 3 - 41.
4. Bernhard Plattner and Hannes Lubich, 'Electronic Mail Systems and Protocols Overview and Case Study, 'Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elsevier Science Publishers B.V., North-Holland, 1989, pp. 55 - 99.
5. Susan Klein Lebeck, 'Implementing MHS: 1984 versus 1988, 'Proceedings of the IFIP TC 6/WG 6.5 Working Conference on Message Handling Systems and Distributed Applications, Costa Mesa, CA., Oct. 1988, Einar Stefferud, Ole J. Jacobsen, and Pietro Schicker, Editors, Elsevier Science Publishers B.V., North-Holland, 1989, pp. 101 - 114.
6. John Linn and Stephen T.Kent, 'Privacy for Dalpa-Internet Mail,' Proceeding of 12th National Computer Security Conference, Washington, D.C., Oct. 1989, pp. 215-229.
7. Matt Bishop, 'Privacy-Enhanced Electronic Mail,' Distributed Computing and

Cryptography: Proceedings of a DIMACS Workshop, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 2, Joan Feigenbaum and Michael Merritt, Editors, American Mathematical Society ACM, Oct. 1989, pp. 93 - 106.

8. Christopher Mitchell, Michael Walker, and David Rush, 'CCITT/ISO Standards for Secure Message Handling,' IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, 1989, pp. 517 - 524.
9. Charles Dinkel, 'SDNS Network, Transport, and Message Security Protocols,' NISTIR 90-44250, U.S. DoC NIST, Gaithersburg, MD, Feb. 1990, pp. 63 - 83
10. Ruth Nelson, 'SDNS Services and Architecture,' Advances in Cryptology-CRYPTO'89 Proceedings (Lecture Notes in Computer Science 435), G. Doos, J. Hartmanis, and G. Brassard, Editors, Springer-Verlag, 1989, pp. 348 - 352.
11. Stephen T. Walker, 'Network Security: The Parts of the Sum,' Proceedings of 1989 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 1989, pp. 2 - 9.
12. Carl Edgar Law, 'X.400 and OSI Electronic Messaging into the 1990s,' IBC Technical Services Ltd., 1989, pp. 76 - 82.
13. Martha Branstad, W. Curtis Barker, and Pamela Cochrane, 'The Role of Trust in Protected Mail,' Proceedings of 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, May 1990, pp. 210-215.
14. Tim Boland, 'Working Implementation Agreements for Open Systems Interconnection Protocols,' U.S. DoC National Institute of Standards and Technology(NIST), Gaithersburg, MD, pp. 6 - 42.
15. Stephen t. Kent, 'Internet Privacy Enhanced Mail,' Communications of the ACM, Vol.36, No.8, Aug. 1993, pp. 48 - 60
16. John McLean, 'Reasoning About Security Models,' Proceedings of 1987 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, Apr. 1987, pp. 123 - 131.