通信情報保護學會論文誌
第 7 卷 第 3 號, 1997. 9

캐스케이드 취약성 방지를 위한 MHS 접근통제 정책 설계

조 인 준*, 김 학 범**, 홍 기 웅***, 김 동 규****

A Design of MHS Access Control Policy for Preventing Cascade Vulnerability

In-June Jo, Hak-Beom Kim, Ki-Yoong Hong, Dong-Kyoo Kim

요 약

다중등급 보안 분산 네트워크 환경에서 MHS(Message Handling System) 보안을 실현하기 위하여 강제적 접근통제(Mandatory Access Control) 정책을 구현한 컴퓨터 시스템들을 상호 연결하였을 때 예기치 않은 캐스케이드 취약성 문제로 인하여 불법적인 정보 흐름이 발생하게 된다

본 논문에서는 이에 대한 해결책으로 캐스케이드 취약성 방지를 위한 새로운 MHS 보안 정책을 제안하고 이를 실현하기 위한 보안 특성 함수를 설계하였다.

Abstract

When computer systems with mandatory access control mechanism are interconnected each other for enforcing the MHS(Message Handling System) security on the multilevel secure distributed network environment, illegal information flow may occurs due to the unexpected cascade vulnerability problem.

In this paper, new MHS security policy and security property functions are proposed for preventing the cascade vulnerability.

1. 서 론

OSI 네트워크 보안 구조에서는 식별/인증, 접근통제, 무결성, 비밀성, 부인방지 등의 보안 서비스를 정의하고 있다. 이러한 보안 서비스들은 암호화, 전자서명, 접근통제, 데이터 무결성, 실체 인증, 트래픽 패딩, 경로 제어, 공증과 같은 여러 가지 메카니즘으로 구현될 수 있

* 배재대학교 컴퓨터공학과 교수
** 한국정보보호센터 선임연구원
*** 한국정보보호센터 책임연구원
**** 아주대학교 컴퓨터공학과 교수

다.[1, 2, 3]

전통적으로 컴퓨터 보안을 실현하기 위한 접근통제 정책으로는 임의적 접근통제(DAC : Discretionary Access Control) 정책과 강제적 접근통제(MAC : Mandatory Access Control) 정책이 제안되었다.[4] 이러한 접근통제 정책중 MAC 정책을 분산 네트워크 환경에서 다중 등급을 갖는 메시지를 보호하기 위하여 적용할 경우 불법적인 정보흐름을 야기시키는 캐스케이드(Cascade) 취약성이 존재함이 밝혀졌다.[5]

캐스케이드 취약성은 MAC 메카니즘이 구현된 서로 다른 컴퓨터 시스템들이 상호 네트워킹되었을 경우 어느 한 시스템에 있는 높은 등급의 정보가 이 시스템과 연결된 낮은 등급의 다른 시스템으로 흘러가는 것으로 정의된다.[5]

분산 네트워크상에서 메시지 보호를 위하여 PGP(Pretty Good Privacy), PEM(Internet Privacy Enhanced Mail), SDNS(Secure Data Network System), MSP(Message Security Protocol) 등의 보안 프로토콜이 개발되었으나 캐스케이드 취약성 방지를 위한 보안 기능은 제공하지 못하고 있는 실정이다.[6, 7, 8, 9, 10, 11]

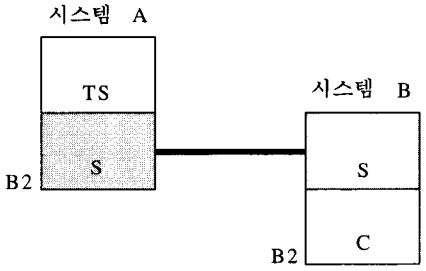
본 논문에서는 분산 네트워크 환경에서 캐스케이드 취약성을 방지하고 다중등급 메시지를 안전하게 처리하기 위한 새로운 캐스케이드 취약성 방지 정책과 보안 특성 함수를 제안한다.

2. MHS 보안 서비스 개념

MHS에 대하여 침입자들이 행하는 유해 행위로는 위장 행위, 메시지 순서 변경, 메시지 정보의 변경, 서비스 부인, 메시지 정보 유출, 부인 등의 다양한 양상으로 나타난다.[12, 13, 14] X.400 권고 안은 MHS보안을 위하여 안전한 접근 관리와 안전한 메시지처리 요구 사항을 기술하고 있다. 안전한 접근 관리는 인접한 MHS구성 요소 간에 인증된 결합(Authenticated Association) 설정을 전제로 이들간에 보안 특성을 표시하는 보안 매개변수를 정의하여 행해진다. 즉 MHS의 UA(User Agent)/MTA (Message Transfer Agent), MTA/MTA, MS(Message Store)/MTA와 같은 각각의 구성 요소 쌍을 대상으로 보안관리가 이루어지도록 정의하고 있다. 또한 MHS 보안 서비스는 이러한 각각의 구성 요소 쌍간의 메시지 제출, 전송, 분배 과정에서 특정 보안 서비스를 지정하는 보안 매개변수를 메시지 처리 과정에 첨가하여 이를 실행시킴에 따라 원하는 보안 서비스를 받을 수 있도록 정의하고 있다.[12]

3. 캐스케이드 취약성

캐스케이드 취약성은 (그림 1)에서 제시한 바와 같이 분산 네트워크 환경에서 MAC 메카니즘이 구현된 서로 다른 컴퓨터 시스템들이 상호 연결되어 있는 경우에 발생한다.[5] 여기에서 B1과 B2는 미국 NCSC에서 컴퓨터 시스템의 보안성 평가를 위하여 제시한 컴퓨터 보안 등급을 각각 의미한다.[4]



TS:Top Secret, S:Secret, C:Confidential

(그림 1) 캐스케이드 취약성이 존재하는 네트워크 환경 예

(그림 1)에서 시스템 A가 처리할 수 있는 데이터에 대한 최고 수준의 비밀 등급은 TS (Top Secret)이고 최저 수준의 비밀 등급은

S(Secret)임을 의미한다. 또한 시스템 B가 처리할 수 있는 데이터에 대한 최고 수준의 비밀 등급은 S이고 최저 수준의 비밀 등급은 C(Confidential)임을 의미한다. 이러한 네트워크 환경에서 시스템 침투자는 시스템 A의 TS 등급의 데이터를 S 등급으로 낮추고 이를 시스템 B로 전송한 후 다시 C 등급으로 낮추는 일련의 침투 공격을 수행함으로써 불법적으로 TS 등급의 데이터를 C 등급의 사용자가 읽어볼 수 있도록 할 수 있다. 이러한 불법적인 정보흐름 문제를 야기시키는 취약성을 캐스케이드 취약성이라고 한다.[5]

4. 다중등급 보안을 위한 MHS 보안정책

4.1 MAC 정책

기존의 MAC정책은 높은 등급의 보안 레이블이 부여된 메시지가 낮은 등급의 보안 레이블을 가진 MHS 사용자 혹은 주체(즉, UA, MTA)에게 전송되는 것을 방지하기 위하여 사용가능하다. 본 절에서는 MHS가 다중등급 메시지를 안전하게 처리할 수 있도록 하기 위하여 필요한 보안 규정들을 기술한다.[17]

- 〈보안 규정-1〉 판독(Read) 접근
  주체의 보안 레이블이 객체의 보안 레이블보다 높은 등급인 경우에만 주체는 객체에 판독 접근할 수 있다.
- 〈보안 규정-2〉 쓰기(Write) 접근
  주체의 보안 레이블이 객체의 보안 레이블에 비하여 높은 등급이 아닐 경우에만 주체는 객체에 대해 쓰기 접근할 수 있다.
- 〈보안 규정-3〉 삭제(Delete) 접근
  주체의 보안 레이블이 삭제할 객체(메시지 혹은 파일)의 보안 레이블과 같고, 메시지 객체를 저장하고 있는 메시지 스풀의 보안 레이블과 같을 때만, 그 객체에 삭제 접근할 수 있다.
- 〈보안 규정-4〉 접속(Connect) 통제
  MHS내의 각 구성 요소(즉, UA, MTA, MS)들 간의 상호 접속은 반드시 보안 레이블이 서로 동일한 경우에만 가능하다. 이는 다중 등급을 갖는 구성 요소간에 예기치 않은 비인가된 정보 흐름을 방지하기 위한 것이다.
- 〈보안 규정-5〉 메시지 제출(Submit) 통제
  발신 주체(즉, 사용자 혹은 발신 UA)는 다음의 조건을 모두 만족하는 경우에만 대응 실체인 주체(즉, MTA)에게 메시지를 제출할 수 있다.
  1) 제출 주체의 보안 레이블이 제출하고자 하는 메시지의 보안 레이블과 서로 동일하다.
  2) 제출 주체의 보안 레이블과 이에 대응하는 대등 실체인 주체의 보안 레이블과 서로 동일하다.
  3) 수신자의 보안 레이블이 메시지의 보안 레이블보다 높은 등급이다.
- 〈보안 규정-6〉 메시지 전송(Transfer) 통제
  주체(즉, MTA)는 다음의 조건을 모두 만족하는 경우에만 이에 대응하는 대등 실체인 다른 주체(즉, MTA)에게 메시지 객체를 전송할 수 있다.
  1) 송신 주체의 보안 레이블과 수신 주체의 보안 레이블이 서로 동일하다.
  2) 송신 주체의 보안 레이블이 메시지 객체의 보안 레이블과 서로 동일하다.
- 〈보안 규정-7〉 메시지 배달(Delivery) 통제
  주체(즉, MTA)는 다음의 조건을 모두 만족하는 경우에만 다른 주체(즉, UA혹은 MS)로 메시지를 배달할 수 있다.
  1) 배달 주체의 보안 레이블은 수신 주체

의 보안 레이블과 서로 동일하다.

2) 배달 주체의 보안 레이블이 메시지의 보안 레이블과 서로 동일하다.

3) 수신자의 보안 레이블은 메시지 보안 레이블보다 등급이 높다.

4.2 캐스케이드 취약성 방지를 위한 새로운 MHS 보안 정책

본 절에서는 MAC 메카니즘을 갖는 컴퓨터 시스템들이 분산 네트워크 환경에서 상호 연결되어 있을 경우 발생가능한 캐스케이드 취약성을 방지하기 위하여 새로운 보안 정책 즉, CFC(Cascade Flow Control) 정책을 제안한다. 먼저 CFC 정책에 필요한 정의를 다음과 같이 정의한다.

정의 1. 보안 등급 ri : 보안 등급 ri는 호스트 시스템 hi에 주어진 보안 등급이고 다음과 같은 조건을 만족한다.

· $r_i \in$ {C1,C2,B1,B2,B3,A1}

· C1 < C2 < B1 < B2 < B3 < A1

단, 여기에서 C1, C2, B1, B2, B3, A1은 미국 NCSC에서 컴퓨터 시스템의 보안성 평가를 위하여 제시한 컴퓨터 보안 등급을 각각 의미한다.[15]

정의 2. 보안 등급 행렬 $T(S_i, C_j)$: 보안 등급 행렬 $T(S_i, C_j)$는 모든 (S_i, C_j)에 대해 컴퓨터 시스템의 보안 등급을 표시한 것으로 다음 조건을 만족한다.

· $\{S_1, S_2, .., S_i, ..., S_a\}$: $1 \le i \le a$인 데이터 비밀 등급의 집합

· $\{C_1, C_2, .., C_j, ..., C_b\}$: $1 \le j \le b$인 사용자 비밀등급의 집합

여기에서 컴퓨터 시스템에 대한 보안 등급 행렬은 [표 1]과 같이 정의된다.[15]

[15]에서 정의된 내용을 토대로 [표 1]을

[표 1] 보안등급 행렬

MDS \ MUC	U	N	C	S	TS(BI)	TS(SBI)	IC	MC
U	C1	C1	C1	C1	C1	C1	C1	C1
N	B1	C2	C2	C2	C2	C2	C2	C2
C	B2	B2	C2	C2	C2	C2	C2	C2
S	B3	B2	B1	C2	C2	C2	C2	C2
TS	*	A1	B3	B2	C2	C2	C2	C2
IC	*	*	A1	A3	B2	B1	C2	C2
MC	*	*	*	A1	B3	B2	B1	C2

설명하면 MUC(Minimum User Clearance)는 시스템 사용자에게 허용된 신원허가 등급중 가장 낮은 신원허가 등급을 의미한다. 사용자의 신원허가 등급은 다음과 같이 분류된다.

- U(Uncleared) : 시스템 내에 저장된 정보중 오직 공개된 정보에 대해서만 접근이 허용됨.
- N(Not Cleared but Authorized to Sensitive Unclassified Information) : 비밀로 분류되지 않은 중요한 정보에 대해서만 접근이 허용됨.
- C(Confidential) : 국가기관의 신원조회를 필한 사람에게 접근이 허용됨을 의미함. 미국의 예를 들면, 미국 시민권자인 경우 이러한 등급의 정보를 참조할 수 있음.
- S(Secret) : 지문조회 등 국가기관의 강화된 신원조회를 필한 사람에게 접근이 허용됨을 의미함.
- TS(BI) : Top Secret(Background Investigation)의 약자로 개인접촉 및 개인기록조회 등을 포함한 국가기관의 신원조회를 필한 사람에게 접근이 허용됨을 의미함.
- TS(SBI) : Top Secret(Special Background Investigation)의 약자로 TS(BI) 신원조회이외에 외국에서 출생한 경우 가족, 이웃사람, 이전 거주지 등을 포함한 국가기관의 신원조회를 필한 사람에게 접근이 허용됨을 의미함.
- 1C(One Category) : TS(SBI) 신원조회 이외

에 하나의 보안 범주(Category)가 허가된 사람에게 접근이 허용됨을 의미함. 예를 들면, 보안관리자의 역할이 부여되는 것이 하나의 범주로 볼 수 있다.

- MC (Multiple Categories) : TS(SBI) 신원조회이외에 여러 개의 보안 범주(Multiple Categories)가 허가된 사람에게 접근이 허용됨을 의미함.

MDS(Maximum Data Sensitivity)는 시스템 내에서 처리되는 데이터에게 부여된 비밀등급중 가장 높은 비밀등급을 의미한다. 데이터의 비밀 등급은 다음과 같이 분류된다.

- U(Unclassified) : 비밀로 분류되지 않은 공개된 일반정보를 의미함.
- N(Not Classified but Sensitive) : 비밀로 분류되지 않은 중요한 정보
- C(Confidential) : 데이터가 불법적으로 노출되었을 때 국가보안에 피해(Damage)를 줄 수 있는 비밀 정보
- S(Secret) : 데이터가 불법적으로 노출되었을 때 국가보안에 심각한 피해(Serious Damage)를 줄 수 있는 비밀 정보
- TS(Top Secret) : 데이터가 불법적으로 노출되었을 때 국가보안 유지가 불가능한 상태(Grave Damage)가 예상되는 비밀 정보
- 1C(One Category) : 단일의 국가 특수보안 분야에 해당되는 TS 정보.
- MC(Multiple Categories) : 여러 개의 국가 특수보안분야에 해당되는 TS 정보.

예를 들어 어느 한 시스템내에 처리되고 있는 데이터의 최대 비밀등급이 TS(Top Secret)이고 사용자의 최소 신원허가 등급이 C(Confidential)이면 [표 1]로부터 이 시스템의 보안성 등급은 B3이어야 함을 알 수 있다.

상기 정의를 토대로 안전한 캐스케이드 경로(Secure Cascade Path)와 취약한 캐스케이드 경로(Vulnerable Casecade Path)를 정의하면 다음과 같다.

정의 3. 안전한 캐스케이드 경로 (i, j) : 네트워크에서 노드가 i, j로 주어질 때, 안전한 캐스케이드 경로 (i, j)는 다음을 만족해야 한다.

· $r_i \geq T(\mathrm{Max}(S_i), \mathrm{Min}(C_j))$ 혹은 $r_j \geq T(\mathrm{Max}(S_i), \mathrm{Min}(C_j))$를 만족해야 한다.

즉, r_i(즉, 노드의 보안 등급) 혹은 r_j(즉, 노드 j의 보안 등급) 중 하나가 노드 i의 최대 데이터 비밀 등급과 노드 j의 최소 사용자 비밀 등급을 조합하여 이를 [표 1]에 적용하여 얻은 컴퓨터 보안 등급과 같거나 높은 등급일 경우 경로 (i, j)는 안전한 캐스케이드 경로이다.

정의 4. 취약한 캐스케이드 경로 (i, j) : 네트워크에서 노드가 i, j로 주어질 때, 취약한 캐스케이드 경로 (i, j)는 다음을 만족해야 한다.

· $r_i < T(\mathrm{Max}(S_i), \mathrm{Min}(C_j))$ 혹은 $r_j < T(\mathrm{Max}(S_i), \mathrm{Min}(C_j))$를 만족해야 한다.

즉, r_i(즉, 노드의 보안 등급) 혹은 r_j(즉, 노드 j의 보안 등급) 중 하나가 노드 i의 최대 데이터 비밀 등급과 노드 j의 최소 사용자 비밀 등급을 조합하여 이를 [표 1]에 적용하여 얻은 컴퓨터 보안 등급 보다 낮은 등급일 경우 경로 (i, j)는 취약한 캐스케이드 경로이다.

다음에서는 위에서 정의한 정의 3과 4를 바탕으로 캐스케이드 취약성 방지를 위한 새로운 보안 정책인 CFC 정책을 제안한다..

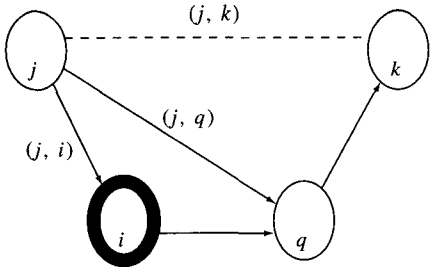
정의 5. CFC 정책 : CFC 정책은 네트워크상에 주어진 노드들에 허가된 컴퓨터 보안 등급 관계를 기반으로 캐스케이드 취약성을 방지하는 정책이다. 이는 다음과 같은 보안 규정을 만족해야 한다.

- 〈보안 규정 8〉 캐스케이드 안전 흐름 (Cascade Secure Flow) 통제
  노드 i는 경로 (j, i)와 (j, q)가 안전한 캐스

케이드 경로일 경우만 노드 q에게 메시지를 전달할 수 있다. 이때 노드 q는 노드 i에서 메시지를 전달할 다음 노드를 의미한다.

이 정책의 개념적인 스킴은 (그림 2)처럼 설명된다.

j와 k는 각각 메시지 발신 노드와 수신 노드이다. i는 현재 메시지가 경유하는 중간 노드이고, q는 메시지가 k의 방향으로 전파될 때, 현재의 i 노드 다음 경유 노드이다. 노드 i의 관점에서, 노드j의 메시지는 경로 (j, i)와 (j, q)가 안전한 캐스케이드 경로(정의 3 참조)일 경우만 노드 i를 경유하여, q에 전송할 수 있다. 따라서 두 경로 (j, i)와 (j, q)에 CFC정책이 적용된다. 다음 노드 q의 관점에서 두 개의 경로 (j, q), (j, k)는 동일한 방법으로 안전한 캐스케이드 경로인지 아닌지를 검사할 수 있다. 이 경우 상기의 두 경로가 안전한 캐스케이드 경로일 경우만 j로부터 q를 경유하여 정보를 전송할 수 있다.



j:발신 노드, k:수신 노드,
i:현재 경유 노드, q:다음 경유노드

(그림 2) CFC 정책 개념

5. 다중 등급 보안을 위한 MHS 보안 특성 함수 설계

본 절에서는 분산 네트워크 환경에서 다중 등급 메시지 처리가 가능하며 캐스케이드 취약성 방지를 위한 MHS 보안 특성 함수의 설계를 제시한다.

5.1 MAC 보안 특성 함수 설계

MAC 보안 특성 함수를 설계하기 위하여 다음의 정의를 이용한다.[17]

· LEVEL : LEVEL(A)는 보안 레이블 A에 포함되어 있는 계층적 분류 정보인 비밀 등급 반환 함수이다.

· COM : COM(A)는 보안 레이블 A에 포함되어 있는 비 계층적 분류 정보인 범주 반환 함수이다.

· dom, eqv : dom(A1, A2)와 eqv(A1, A2)는 2개의 보안 레이블간의 지배관계를 나타낸 함수로 2개의 보안 레이블 A1과 A2에 대하여 다음과 같이 정의 된다.

```
dom(A1, A2)
begin
 if LEVEL(A1)≥( LEVEL(A2) .and.
 COM(A1)⊇COM(A2) then return TRUE ;
                    else return FALSE;
end

eqv(A1, A2)
begin
 if dom(A1, A2) .and. dom(A2, A1)
        then return TRUE;
        else return FALSE;
end
```

상기의 정의를 이용하여 MAC 보안 특성 함수를 설계하면 다음과 같다. MAC 보안 특성은 BLP 모델에서 제시한 단순 보안 특성(SS : Simple Security Property)과 스타 보안 특성(* : Star Property)으로 구성된다.[4, 16] 그리고 추가적으로 일치 보안 특성(Compatibility Security

Property)으로 "compat", 접속 보안 특성(Connect security property)으로 "cons"를 사용한다. 여기에서 사용된 기호는 다음과 같은 의미를 갖는다. S는 주체(MHS-에이전트 혹은 MS), O는 객체(메시지 혹은 파일), M은 접근 모드 집합{'r','w','d'}, m은 S가 O에게 요구한 접근 모드, CSL은 S의 현재 보안 레이블, SL은 객체 O의 보안 레이블, H(O)는 객체의 트리 계층에서 객체 O의 깊이 등급(Depth level) 값을 반환하는 함수를 각각 나타낸다.

· ss : ss(S, O, m)는 단순 보안 특성 함수로 다음과 같이 정의되며 상향 판독 금지(No read-up)를 위한 보안 특성 함수임을 의미한다.

```
ss(S, O, m)
begin
 if m ∈ M .and. dom(CSL(S), SL(O))
    then return TRUE;
    else return FALSE;
end
```

· star : star(S, O, m)은 스타 보안 특성 함수로 다음과 같이 정의되며 하향 쓰기 금지(no write-down)를 위한 보안 특성 함수임을 의미한다.

```
star(S, O, m)
begin
 if m = 'r' .and. dom(CSL(S), SL(O))
              then return TRUE;
    elseif m = 'w' .and. dom(SL(O), CSL(S))
              then return TRUE;
    elseif m = 'd' .and. eqv(CSL(S), SL(O))
              then return TRUE;
    else return FALSE;
end
```

· compat : compat(O1, O2)는 일치성 보안 특성 함수로 다음과 같이 정의되며 객체 계층에서 객체 O1과 O1의 부모 객체 O2간에 보안 레이블의 일치성 유무를 결정하여 이의 결과 값(참 또는 거짓)을 반환하는 함수이다.

```
compat(O1, O2)
begin
 if H(O2) > H(O1) .and. eqv(SL(O1), SL(O2))
        then return TRUE;
        else return FALSE;
end
```

· cons : cons(S1, S2)는 접속 보안 특성 함수이다. 이는 통신 실체(혹은 주체)간에 안전한 접속 유무를 결정하여 이의 결과 값(참 또는 거짓)을 반환하는 함수이다. 이 특성은 주체(즉, MHS-에이전트 혹은 MS) S1의 현재 보안 레이블이 S2의 보안 레이블과 같을 경우만 안전한 접속을 이룰 수 있음을 의미한다.

```
cons(S1, S2)
begin
 if eqv(CSL(S1), CSL(S2)) then return TRUE;
                          else return FALSE;
end
```

5.2 캐스케이드 취약성 방지를 위한 보안 특성 함수 설계

본 절에서는 4장에서 제안한 CFC 정책을 수행하기 위하여 CFC 보안 특성 함수의 설계를 제안한다. 먼저 다음의 기호를 추가로 정의한다.

- r : $r(i)$는 노드 i의 컴퓨터 보안 등급을 반환하는 함수이다.
- AR : AR(i)는 노드 i가 처리할 수 있는 비밀 등급의 범위를 반환하는 함수이다.
- CS(Cascade Secure) : CS(S1, S2)는 노드 S1과 S2에 대해, 캐스케이드 취약성 유.무를 검사하는 함수이다. 이 함수가 참 값을 반환하면 안전한 캐스케이드 경로에 의한 메

시지 흐름이 되고, 거짓 값을 반환하면 캐스케이드 취약성이 존재함을 뜻한다. CS 함수는 다음과 같이 정의된다.

```
CS(S1, S2)
begin
 if r(S1)≥( T(Max(AR(S1)), Min(AR(S2)))
   .or. r(S2)≥( T(Max(AR(S1)), Min(AR(S2)))
      then return TRUE;
      else return FALSE;
end
```

위의 정의를 토대로 캐스케이드 취약성 방지를 위한 캐스케이드 흐름 보안(cfs : Cascade Flow Security) 특성 함수를 제안하면 다음과 같다.

- cfs : cfs(S1, S2, S3)는 노드 S1, S2, S3가 주어졌을 때 S1이 S2를 경유하여 S3로 안전한 경로를 유지하는지를 판단하는 함수이다. 이 함수가 참 값을 반환하면 S1과 S3사이의 경로는 캐스케이드 취약성이 존재하지 않는 안전한 경로임을 의미한다. 그렇지 않을 경우에는 S1과 S3 사이의 경로는 캐스케이드 취약성이 존재함을 의미한다.

```
cfs(S1, S2, S3)
begin
 if CS(S1, S2) .and. CS(S1, S3)
       then return TRUE;
       else return FALSE;
end
```

따라서 cfs(S1, S2, S3)가 참 값을 반환할 경우에는 노드 S1에서 노드 S2를 경유하여 노드 S3로 메시지가 전송될 수 있다. 이때, S2는 MTA와 같은 중계 노드가 된다.

5.3. 보안 정책과 보안 특성 함수와의 관계

제4장에서 제안한 보안 정책과 본 장에서 제안한 보안 특성 함수간의 관계를 정리 하면 [표 2]와 같다. 기호 "•"는 이들 사이에 관계가 있음을 표시한 것이다.

[표 2] 보안 정책과 보안 특성 함수간의 관계

보안 정책 \ 보안 특성 함수		ss	star	cons	compat	cfs
MAC	1. Read Access	•	•			
MAC	2. Write Access	•	•		•	
MAC	3. Delete Access	•	•			
MAC	4. Connect			•		
MAC	5. Submit	•	•		•	•
MAC	6. Transfer	•	•		•	•
MAC	7. Deliver	•	•		•	•
MAC	8. Cascade Secure Flow					•

즉, MHS가 메시지에 대하여 쓰기 접근을 안전하게 수행하기 위해서는 ss, star, compat 보안 특성을 만족해야 하며, 캐스케이드 취약성으로 인하여 메시지가 불법적으로 유출되지 않도록 하기 위해서는 cfs 보안 특성을 만족해야 함을 의미한다.

6. 결 론

분산 네트워크 환경에서 MAC 메카니즘을 구현한 컴퓨터 시스템들이 상호 연결될 경우 캐스케이드 취약성이 존재할 수 있다.

본 논문에서는 이러한 캐스케이드 취약성을 방지하기 위한 MHS 보안 정책을 새롭게 제안하였고, 제안된 보안 정책을 위한 보안 특성 함수를 설계하였다. 이러한 보안 정책과 보안 특성 함수는 분산 네트워크 환경에서 다중 등급의 메시지를 안전하게 처리하기 위한 MHS의 설계 및 구현에 응용될 수 있다.

향후에는 본 논문에서 캐스케이드 방지를 위하여 새롭게 제안한 보안 정책과 보안 특성 함수를 기반으로 캐스케이드 취약성 방지 메

카니즘의 설계 및 구현을 통하여 캐스케이드 취약점이 없는 안전한 MHS 시스템 구현으로 이어질 것이다.

참 고 문 헌

[1] ISO/IEC 7498-2, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2 : Security Architecture, Feb. 1989.

[2] Dennis K. Branstad, "Considerations for Security in the OSI Architecture", IEEE Network Magazine, Vol.1, No.2, pp.34-39, Apr. 1987.

[3] Marshall D. Abrams and Albert B. Jeng, "Network Security: Protocol Reference Model and the Trusted computer System Evaluation Criteria," IEEE Network Magazine, Vol. 1, No, 2, pp. 24 - 33, Apr. 1987.

[4] 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.

[5] National Computer Security Center, "Trusted Network Interpretation of the Department of Defense Trusted Computer System Evaluation Criteria,"NCSC-TG-005, Version-1, July 31, 1987.

[6] Larry J. Hughes, Jr., Actually Useful Internet Security Techniques, New Rider Publishing, 1995.

[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, pp. 93 - 106, Oct. 1989.

[8] 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, pp. 210 - 215, May 1990.

[9] Charles Dinkel, "SDNS Network, Transport, and Message Security Protocols," NISTIR 90-44250, U.S. DoC NIST, Gaithersburg, MD, Feb. 1990.

[10] John Linn and Stephen T.Kent, "Privacy for Dalpa-Internet Mail," Proceeding of 12th National Computer Security Conference, Washington, D.C., pp. 215-229, Oct. 1989.

[11] Stephen T. Kent, "Internet Privacy Enhanced Mail," Communications of the ACM, Vol.36, No.8, pp. 48 - 60, Aug. 1993.

[12] CCITT, Data Communication Networks Message Handling Systems, CCITT Recommendations, X.400-X.420, Nov.1988.

[13] M. J. Gosselin, "Message Handling Systems (X.400) Threats, Vulnerabilities, and Countermeasures," Proceedings of the

13th National Computer Security Conference, Baltimore, MD, pp. 226 - 235, Oct. 1993.

[14] 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, pp. 517 - 524, 1989.

[15] National Computer Security Center, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments," CSC-STD-004-85, June 25, 1985.

[16] D.E. Bell, "Secure Computer Systems : A Refinement of the Mathematical Model," MITRE, ESD-TR-73-278, Vol. III, pp. 5 - 39, Apr. 1974.

[17] 홍기웅, 임병렬, 김동규, "메시지 처리 시스템의 안전한 정보흐름을 위한 네트워크 액세스 제어 메커니즘의 설계," 통신정보보호학회 논문지, Vol. 4, No. 2, pp. 89 - 112, Dec. 1994.

□ 著者紹介

조 인 준

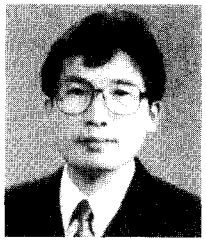
1982. 2 전남대학교 전자계산학과 졸업(학사)
1985.2 전남대학교 전자계산학과 대학원 졸업(석사)
1997.10 - 현재 아주대학교 컴퓨터공학과 박사과정 재학중
1990. 12 정보처리기술사(전산 조직 응용)
1983.9 - 1994.2 한국전자통신연구소 선임연구원
1994.3 - 현재 배재대학교 컴퓨터공학 교수

※ 관심분야 : 전산 조직응용 및 정보통신 Security

김 학 범

1988.2 경기대학교 전자계산학과(학사)
1990.8 중앙대학교 대학원 전자계산학과(석사)
1996.3 - 현재 아주대학교 대학원 컴퓨터공학과 박사과정 재학중
1991.10 - 1996.6 한국전산원 주임연구원
1996.7 - 현재 한국정보보호센터 선임연구원

※ 관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호기술 표준화



홍 기 융

1985.2 전남대학교 전자계산학과(학사)
1990.2 중앙대학교 대학원 전자계산학과(석사)
1996.2 아주대학교 컴퓨터공학과(박사)
1985. 9 - 1995.10 한국전자통신연구소 선임연구원
1992.9 - 1993.6 이탈리아 Alenia spazio S. P. A 선임연구원
1994.8 정보처리기술사
1995.10 - 1996.4 한국전산원 선임연구원
1996.4 - 현재 한국정보보호센터 책임연구원, 평가체계팀장

※ 관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가체계, 정보보호기술 표준화

김 동 규

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(Ph.D. 전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1979.3 - 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이타 통신시스템, 희중당, 1986년
저서 : 컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 한국통신정보보호학회 부회장

※ 관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템